

BETWEEN:

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant and Defendant to Counterclaim

-and-

FARHAD AZIMA

Defendant and Counterclaimant

-and-

STUART ROBERT PAGE

First Additional Defendant to Counterclaim

-and-

DAVID NEIL GERRARD

Second Additional Defendant to Counterclaim

-and-

DECHERT LLP

Third Additional Defendant to Counterclaim

-and-

JAMES EDWARD DENNISTON BUCHANAN

Fourth Additional Defendant to Counterclaim

**DEFENCE OF THE DEFENDANT
TO THE RE-AMENDED COUNTERCLAIM**

PRELIMINARY

1. Except where expressly stated, references to paragraph numbers are to paragraphs of the Re-Amended Counterclaim. For convenience of reference only, and without thereby making any admission, the Defendant to the Counterclaim ("**RAKIA**") adopts the headings and definitions contained in the Re-Amended Counterclaim. Unless specifically admitted or not admitted below, RAKIA joins issue with the Counterclaimant ("**Mr Azima**") on the Re-Amended Counterclaim.

I. THE PARTIES

2. Paragraphs 1 and 2 are admitted. Following a four-week trial between 22 January and 14 February 2020 (“the **First Trial**”), Mr Andrew Lenon QC (“the **Judge**”) delivered a judgment dated 22 May 2020 ([2020] EWHC 1327 (Ch)) (“the **Judgment**”) in which he held that Mr Azima had engaged in a wide range of “*seriously fraudulent conduct*” towards RAKIA. In particular, the Judge found that:
 - 2.1. Mr Azima had induced RAKIA to enter into a settlement agreement dated 2 March 2016 (“the **Settlement Agreement**”) by means of:
 - (a) a fraudulent misrepresentation concerning the amount of an investment made by Mr Azima’s company, HeavyLift International Airlines FZC (“**HeavyLift**”) in a joint venture with RAKIA (“the **HeavyLift Investment Misrepresentation**”); and
 - (b) a fraudulent misrepresentation that Mr Azima had always acted in good faith towards RAKIA and its related entities (“the **Good Faith Misrepresentation**”);
 - 2.2. Mr Azima had engaged in an unlawful means conspiracy against RAKIA in connection with the intended sale of a luxury hotel (“the **Hotel**”) in Tbilisi, Georgia, in the course of which Mr Azima:
 - (a) falsely claimed to have introduced the proposed buyers of the Hotel to RAKIA and, on the basis of that false claim, misappropriated \$1,562,500 from RAKIA; and
 - (b) manufactured a sham contract (“the **Sham Referral Agreement**”) designed to conceal his dishonest misappropriation of funds from RAKIA;
 - 2.3. Mr Azima paid a bribe of \$500,000 to RAKIA’s former chief executive, Dr Khater Massaad;
 - 2.4. Mr Azima had overseen the commissioning of and payment for a “Security Assessment” report, which advocated using various unlawful means (including “*scams, frauds and deceptive partnerships*”) to inflict significant financial and reputational damage against various RAK institutions and companies; and
 - 2.5. Mr Azima had made fraudulent representations to RAKIA in negotiations for a proposed intelligence, surveillance and reconnaissance joint venture (“the **Proposed ISR Joint Venture**”).

3. As to paragraph 3:

- 3.1. It is admitted that Mr Stuart Page is an investigator who operates, inter alia, in the Middle East. It is denied that Mr Page was RAKIA's agent. RAKIA did not, at any time, confer authority on Mr Page to act on its behalf.
- 3.2. It is admitted that Mr Neil Gerrard is a solicitor. Mr Gerrard was a partner at the international law firm Dechert LLP ("**Dechert**") until his retirement in late 2020. Mr Gerrard was not engaged by RAKIA in his personal capacity.
- 3.3. From 2012, RAKIA engaged Dechert to provide legal advice and assistance in relation to a number of matters ("the **Dechert Retainer**").
- 3.4. It is admitted that Mr James Buchanan was the Chief Executive Officer of Ras Al Khaimah Development LLC ("**RAK DEV**") until his retirement in late 2019. Mr Buchanan was first engaged by RAK DEV in September 2014. RAK DEV was responsible (amongst other things) for holding and managing various assets such as shares, properties and loans which were previously owned by RAKIA. This included assets which were the subject of significant frauds and other wrongdoing committed by RAKIA's former Chief Executive Officer, Dr Khater Massaad. It is admitted that, from November 2014, Mr Buchanan was authorised by RAKIA to undertake various activities on its behalf in connection with such assets and RAKIA's previous business dealings.
- 3.5. As to subparagraph (e):
 - (a) It is admitted that insofar as Mr Buchanan was acting as the directing mind and will of RAKIA, RAKIA is primarily liable for his acts and omissions.
 - (b) It is denied that RAKIA is "primarily" liable for the alleged acts and omissions of the other Additional Defendants.
 - (c) It is admitted that RAKIA is vicariously liable for the acts and omissions of Mr Buchanan while he was acting within the scope of his authority to act on behalf of RAKIA.
 - (d) It is admitted that RAKIA is vicariously liable for the acts and

omissions of Mr Gerrard and Dechert while they were acting on the instructions of RAKIA within the scope of the Dechert Retainer.

(e) It is denied that RAKIA is vicariously liable for the acts and omissions of Mr Page.

(f) It is denied that RAKIA is responsible for the wrongs alleged in the Re-Amended Counterclaim.

3.6. Allegations in the Re-Amended Counterclaim to the effect that RAKIA has acted or failed to act in specified ways are understood to be allegations as to the actions or omissions of RAKIA's "directing mind" or authorised agents acting within the scope of their authority. RAKIA's response to such allegations is a response in relation to the actions or omissions of such persons and this Defence to Counterclaim should be construed accordingly.

3.7. With the exception of the above, paragraph 3 is not admitted.

4. Save that it is denied that RAKIA has sought to conceal any of the matters which are the subject of Mr Azima's claim, the first sentence of paragraph 4 is not admitted. RAKIA does not plead to the second sentence as it does not contain any relevant averment.

II. BACKGROUND AND PROCEDURAL CONTEXT

5. As to paragraph 5:

5.1 It is admitted that at some time prior to 4 August 2016, several of Mr Azima's email accounts were accessed without his authority. The date(s) when, and the means by which, the unauthorised access to those email accounts occurred and the identity of the persons responsible for this are outside RAKIA's knowledge.

5.2 No admissions are made concerning Mr Azima's alleged lack of knowledge of the unauthorised access.

5.3 If and insofar as it is so alleged, it is denied that Mr Azima did not suspect there had been any unauthorised access to his email accounts prior to the publication of the hacked data in August 2016. In support of this, RAKIA will rely on the fact that on various dates in 2015 and 2016 Mr Azima and his close associates and employees,

Mr Ray Adams and Ms Afsaneh Azadeh, and Mr Azima's lawyer in the United States, Mr Kirby Behre, expressed the belief or suspicion that certain of Mr Azima's email accounts had been accessed by an unknown third party/parties. In support of this RAKIA will rely on the following messages sent by Mr Azima, Mr Adams, Ms Azadeh and Mr Behre:

- (a) On 16 October 2015, Mr Azima received an email from a MESVR email address. He forwarded this to Mr Behre, who in turn forwarded it to an IT specialist. The IT specialist responded by highlighting the MESVR feature and explaining that the email was "*a fake message*" and that, "*The sender domain is mesvr.com... this site is associated with a web service named ReadNotify.com that is used to track when someone reads your email.*" Mr Behre forwarded this explanation to Mr Azima and stated that the MESVR message "*may have been a set up to make sure you read it... or perhaps a worm to infiltrate your email*".
- (b) On 28 November 2015, Ms Azadeh received a message from a MESVR email address purporting to be from Mr Azima. She forwarded the email to Mr Azima stating: "*Everyday I have some strange emails from you. I guess all your emails are infected.*" Mr Azima forwarded the exchange to Mr Adams asking: "*Am I infected?*" Mr Adams replied that the MESVR email was a form of attempted "*spoofing*" whereby the "*spoofers...are trying to get the recipient to double click the attachment which contains the virus or malware*".
- (c) On 28 January 2016, Mr Behre sent an email to Mr Adams stating that Mr Adams had received an email containing "*a very powerful virus*" and advising him to "*get your system scrubbed as we are doing*". Mr Behre forwarded the warning to Mr Azima and stated: "*Your email may be compromised too*".
- (d) On 9 February 2016, Mr Behre sent an email to Mr Azima with the subject line "*you just opened the infected document Ray 'sent' to me on your HH account*". In response to Mr Azima's reply to that message, Mr Behre warned Mr Azima that "*the HH*

account may have been infected". The references to the "HH account" were references to the pseudonymous hh@fathers.church email account used by Mr Azima.

- (e) On 29 March 2016, Mr Azima sent an email to Mr Behre stating: *"Ray, Kirby thinks my email maybe hacked? How do you find out?"*
- (f) On 12 April 2016, Mr Azima sent an email to Mr Adams which showed that a third party had managed to send spam messages from his farhad@farhadazima.com email account. Mr Azima's email stated: *"Looks like I am hacked"*.
- (g) On 31 May 2016, Mr Azima sent an email to two employees of the Waldorf Astoria stating: *"My fa@farhadazima.com <mailto:fa@farhadazima.com> was and is probably Hacked! Someone keep changing my password and I can't access the account. Please use my other email address: fa1. For security reasons I am not giving the full info but will email you from other account."*
- (h) On 10 June 2016, Mr Azima sent another email to Mr Adams which again showed that a third party had managed to send spam messages from his farhad@farhadazima.com email account. Mr Azima stated: *"Ray, does this means [sic] my email act [sic] is hacked again?"*
- (i) On 12 June 2016, Mr Azima sent a further email to Mr Adams which showed another spam message had been sent by a third party from his farhad@farhadazima.com email account. Mr Azima stated: *"Hacked again!"*

6. As to paragraph 6:

- 6.1. It is admitted that approximately 30GB of Mr Azima's data was made available via BitTorrent links on the internet in August and September 2016 ("the **hacked data**").
- 6.2. No admissions are made as to the further (unspecified) publications relied on.
- 6.3. It is not admitted that any of the hacked data (or any other data allegedly made available online) was private or confidential to Mr

Azima. Further:

- (a) The hacked data contained a significant volume of documents which were created, sent or received by Mr Azima in the course of committing serious wrongdoing and/or which constituted evidence of such wrongdoing (“the **Iniquity Documents**”). The Iniquity Documents and the information which they contained were not private or confidential to Mr Azima. In support of this averment, RAKIA will rely on the principle that there is no confidence or reasonable expectation of privacy in iniquity. RAKIA will also rely on:
 - (i) The extensive findings of fraud, bribery and other wrongdoing and dishonesty made against Mr Azima contained in the Judgment.
 - (ii) The conclusion of the Court of Appeal at paragraph 47 of its judgment dated 12 March 2021 ([2021] EWCA Civ 349) that: *“the materials which were obtained through hacking Mr Azima’s email accounts...revealed serious fraud on the part of Mr Azima which would have been a very serious bar to the grant of equitable relief in his favour”*.
- (b) Further:
 - (i) A substantial proportion of the hacked data consisted of communications between Mr Azima or those acting on his behalf with RAKIA and related entities (“the **RAKIA Communications**”). Mr Azima did not have any expectation of privacy or confidence vis-à-vis RAKIA or its agents in relation to the RAKIA Communications.
 - (ii) A substantial further proportion of the hacked data consisted of generic and unsolicited advertising and spam email messages which did not contain any information about or relating to Mr Azima (“the **Generic Messages**”). Mr Azima did not have any expectation of privacy or confidence in respect of the Generic Messages.

7. Save that RAKIA’s claim for conspiracy was not part of RAKIA’s original pleaded case served on 30 September 2016, but rather was advanced for

the first time in RAKIA's Amended Particulars of Claim dated 11 December 2017, paragraph 7 is admitted.

8. Paragraph 8 is admitted.
9. Paragraph 9 is admitted.
10. Paragraph 10 is admitted. RAKIA will refer at trial to the Judgment and the Judge's order for their full terms.
11. Paragraph 11 is admitted. RAKIA will refer at trial to the Court of Appeal's order for its full terms.
12. Save that no admissions are made as to Mr Azima's intentions, paragraph 12 is admitted.
13. RAKIA does not plead to paragraph 13 as it contains no relevant averments.
14. As to paragraph 14:
 - 14.1. It is admitted that the hacking was covert in that the person or persons responsible have not made their involvement public.
 - 14.2. It is denied that RAKIA conspired with the Additional Defendants (or anyone else) to cover up and conceal the "*true facts*".
 - 14.3. If and insofar as it is alleged that the "*true facts*" are the factual matters in relation to hacking set out in the Re-Amended Counterclaim, this allegation is denied.
15. As to paragraph 15:
 - 15.1. Subparagraph a. is admitted. The dispute stemmed from RAKIA's discovery that Dr Massaad had systematically defrauded RAKIA over a period of years, and RAKIA's attempts to pursue redress from Dr Massaad in respect of those frauds. Further details are provided at paragraph 28 below.
 - 15.2. Subparagraphs b. to f. are a summary of contentions which are repeated and developed at greater length in later sections of the Re-

Amended Counterclaim. RAKIA's response to those contentions is set out in the sections of this Defence to the Counterclaim which respond to those sections of the Re-Amended Counterclaim. To avoid unnecessary repetition, RAKIA does not plead a separate response to the summary of contentions contained at subparagraphs b. to f.

- 15.3. Save that it is not admitted that any of the hacked data was confidential or private, subparagraph g. is admitted. RAKIA was not responsible for making available the hacked data via the torrent sites ("the **Torrents**") and does not know who was responsible for this.
16. Paragraph 16 contains a summary of contentions which are repeated and developed at greater length in later sections of the Re-Amended Counterclaim. RAKIA's response to those contentions is set out in the sections of this Defence to Counterclaim which respond to those sections of the Re-Amended Counterclaim. To avoid unnecessary repetition, RAKIA does not plead a separate response to the summary of contentions in paragraph 16.
17. Paragraph 16 above is repeated in relation to paragraph 17, making the necessary changes.
18. As to paragraph 18:
- 18.1. It is admitted that following the delivery of the Judgment, Mr Azima claimed that searches conducted after the First Trial had identified more than 150 emails received by Mr Azima and others associated with him between 2015 and 2018, which Mr Azima contended pointed to a single hacking campaign targeting Mr Azima and those individuals. No admissions are made regarding the timing and circumstances of the searches which led to the location of those emails.
- 18.2. It is denied that all of the emails identified by Mr Azima had false content tailored specifically to the recipients. The majority of the emails were generic spam or phishing emails which did not contain content which was tailored specifically to the recipients.
- 18.3. It is admitted that some (but not all) of the emails identified by

Mr Azima had some common technical features.

- 18.4. It is denied that any of the features of the emails identified by Mr Azima indicated that they were all part of a single 'spear-phishing' campaign targeting Mr Azima and others associated with him.
 - 18.5. Further details of RAKIA's case regarding these emails are provided at paragraphs 53 to 56 below.
19. The Re-Amended Counterclaim has abandoned, without explanation, the contention previously advanced at paragraph 19 of the Amended Counterclaim.
20. As to paragraph 20:
- 20.1. It is admitted that documents purporting to be bank statements of CyberRoot Risk Advisory Private Limited ("**CyberRoot**") were disclosed (in redacted form) in other proceedings in January 2021 and that those documents showed that over \$1 million had been paid to CyberRoot between 2015 and 2017 by Vital Management Services ("**Vital**"), a company controlled by Mr Nicholas del Rosso.
 - 20.2. No admissions are made as to the authenticity or accuracy of the bank statements or as to the circumstances in which they were revealed.
 - 20.3. It is admitted that CyberRoot is a company based in India.
 - 20.4. As to the payments referred to, from early 2015, Vital was engaged by Dechert on behalf of RAK DEV to assist investigations into assets in India which had been stolen from RAKIA and the Government of RAK. In 2015 and 2016, Vital engaged CyberRoot to provide various IT, data security and forensic data recovery and analysis services including work in support of that investigation. In addition, in late 2016 and early 2017, Vital engaged CyberRoot to undertake online reputation management work investigating websites which contained material damaging to the reputation of individuals associated with RAK. Between 2015 and 2017 Vital also engaged CyberRoot to undertake work for clients other than RAK DEV.
 - 20.5. It is denied that any of the payments to CyberRoot by Vital on behalf of RAK DEV related to work that concerned Mr Azima or involved any instructions to engage in computer hacking or disseminating material

obtained through hacking.

21. As to paragraph 21:

- 21.1. Mr Buchanan was the owner and director of Gravitas International FZE. Mr Buchanan has never owned or had any involvement with a company named Gravitas International LLC (“**Gravitas**”).
- 21.2. No admissions are made as to the authenticity of the documents referred to in paragraph 21.
- 21.3. It is not admitted that those documents accurately record payments to CyberRoot by Gravitas.

22. As to paragraph 22:

- 22.1 It is admitted that in a witness statement dated 11 February 2021 Mr Jonas Rey states that he was informed by a former CyberRoot employee named Vikash Kumar Pandey that he and others at CyberRoot had hacked Mr Azima’s computers and emails on the instruction of Vital.
- 22.2 The evidence which Mr Rey records as being provided by Mr Pandey is implausible and unreliable. In particular:
 - (a) Mr Rey’s claim in his witness statement that Mr Pandey (with whom he had apparently had no previous contact) was “*forthcoming*” and “*boastful*” about his alleged involvement in hacking is inherently implausible.
 - (b) Mr Azima’s solicitors failed to disclose that several months before the date of Mr Rey’s statement they had been in direct contact with Mr Pandey and that during the course of their communications with Mr Pandey they had (i) threatened Mr Pandey with litigation and offered him “*a single opportunity to co-operate*” with Mr Azima in order to avoid proceedings being brought against him; (ii) offered to pay Mr Pandey substantial sums of money (potentially more than \$16,000 per month) in exchange for the provision of ongoing “consultancy” “services” in support of Mr Azima’s case against RAKIA; and (iii) produced and sent to Mr Pandey a draft “*Consultancy Agreement*” enshrining this proposed arrangement.

- (c) According to Mr Rey, his oral discussion with Mr Pandey took place through two intermediaries (one of whom is anonymous) who acted as interpreters of Mr Rey's questions to Mr Pandey and of Mr Pandey's answers to those questions. Written messages which allegedly emanated from Mr Pandey were also transmitted to Mr Rey indirectly via those intermediaries. Neither of those intermediaries has provided a witness statement. Accordingly, Mr Rey's evidence about what he was allegedly told by Mr Pandey is uncorroborated multiple hearsay about statements allegedly made in a foreign language.

22.3 Save as set out above, paragraph 22 is not admitted.

22A. As to paragraph 22A:

22A.1 No admissions are made regarding the alleged expertise or activities of Aditya Jain or Cyber Defence and Analytics or Mr Jain's alleged ownership of Cyber Defence and Analytics.

22A.2 No admissions are made regarding the existence, content or accuracy of any alleged admissions made by Mr Jain.

23. As to paragraph 23:

23.1. Vital was instructed by Dechert to carry out work for RAK DEV in connection with an investigation into assets misappropriated from RAKIA and the RAK Government and in connection with certain related online reputation management work. Paragraph 20.4 above is repeated.

23.2. It is admitted that Mr del Rosso and Vital were instructed by Dechert on behalf of RAK DEV to arrange for the download of the hacked data via the Torrents.

23.3. It is denied that Vital was instructed to carry out work for RAKIA at any relevant time. It is further denied that Vital provided instructions to CyberRoot for or on behalf of RAKIA.

24. Paragraph 24 is admitted as a summary of the relevant proceedings between Mr Al Sadeq and Mr Gerrard, Dechert, Mr Hughes and Ms Black ("the **Al Sadeq Proceedings**") and the proceedings between Stokoe Partnership

Solicitors and Mr Paul Robinson, Mr Oliver Moon, Mr Patrick Grayson and Mr Page.

25. As to paragraph 25:

25.1. It is denied that Mr Grayson provided services to RAKIA (whether through GPW or otherwise) in regard to “the RAK Project”. There was no such project.

25.2. Mr Grayson did not provide services to RAKIA (whether through GPW or otherwise) in regard to the investigations into Dr Massaad and his associates in or before 2016. Accordingly, RAKIA was not under any obligation to identify Mr Grayson as providing investigative services to RAKIA in or before 2016, and it did not do so.

25.3. No admissions are made regarding the alleged introduction of Mr Jain to Mr Grayson in August 2019 or any “*indica[ti]on*” allegedly provided by Mr Grayson to Mr Jain.

25.4. No admissions are made regarding any “*investigation*” being undertaken by or on behalf of Mr Azima or in respect of Mr Azima’s intention regarding any future application to join Mr Grayson as a defendant.

26. Paragraph 26 is admitted.

27. RAKIA does not plead to paragraph 27 as it contains no relevant averments.

III. THE HACKING

A. THE “RAK PROJECT”

28. As to paragraph 28:

28.1. Dr Massaad was RAKIA’s chief executive officer between 2005 and 2012. In 2012, RAKIA discovered that Dr Massaad had engaged in systematic wrongdoing and, in conjunction with various others, had conspired to defraud RAKIA and other RAK-owned entities of assets worth hundreds of millions of dollars.

28.2. Dr Massaad absconded from RAK and was subsequently tried, convicted and sentenced *in absentia* for an array of fraud,

embezzlement and bribery offences.

28.3. Following the discovery of Dr Massaad's frauds, RAKIA sought to engage in negotiations with Dr Massaad and his representatives with a view to locating and recovering the assets misappropriated by Dr Massaad and his criminal associates. In the context of those negotiations, Dr Massaad made false assertions that he was owed sums in connection with his work as RAKIA's chief executive.

28.4. Subject to the above, paragraph 28 is admitted.

29. Paragraph 29 is admitted.

30. Paragraph 30 is denied. The term "the RAK Project" was not generally used to describe the investigations into Dr Massaad and the persons associated with him.

B. RAKIA'S AGENTS

31. As to paragraph 31:

31.1. It is admitted that RAKIA engaged Dechert to provide legal advice and assistance in connection with its disputes with Dr Massaad and his associates.

31.2. RAKIA did not separately engage any individual partners of Dechert.

32. As to paragraph 32:

32.1. It is denied that RAKIA engaged the persons listed in subparagraphs a. to d. as alleged in paragraph 32.

32.2. The persons listed were engaged as follows:

(a) Mr Page was engaged on behalf of the Ruler and the Government of RAK.

(b) From around September 2014 Mr del Rosso and Vital were engaged by Dechert on behalf of RAK DEV to undertake work relating to the investigation of assets stolen from RAKIA and/or the Government of RAK. Paragraph 20 above is repeated. In addition, in August and September 2016 Mr del Rosso and Vital were engaged by Dechert on behalf of RAK DEV to assist in retrieving the hacked data from the internet.

- (c) Karv Communications was not engaged by RAKIA (whether directly or indirectly) or any other RAK related entity to investigate or gather information about Dr Massaad or anyone else. At all relevant times, Karv Communications provided advice on public relations and media management. Mr Andrew Frank was an employee of Karv Communications and Mr Amir Handjani was a senior adviser to the company.
- (d) RAKIA did not, at any relevant time, engage Mr Grayson (whether through GPW or otherwise) to investigate or gather information from and about Dr Massaad and his associates.

32.3. With the exception of the above, paragraph 32 is not admitted.

33. As to paragraph 33:

33.1. It is admitted that from late 2014 Mr Buchanan was engaged by RAK DEV to deal with certain of RAKIA's affairs.

33.2. It is admitted that Mr Buchanan had authority to take steps on RAKIA's behalf.

33.3. With the exception of the above, paragraph 33 is denied.

34. As to paragraph 34:

34.1. It is admitted that Mr Buchanan provided instructions to Mr Gerrard (on behalf of Dechert) in relation to legal advice and assistance which fell within the scope of the Dechert Retainer.

34.2. It is denied that Mr Gerrard provided instructions to Mr del Rosso and Vital on behalf of RAKIA. Paragraph 32.2(b) above is repeated.

34.3. It is denied that Mr Buchanan or Mr Gerrard provided instructions to Mr Page (and, through Mr Page, his company Stuart Page MEFZ) on behalf of RAKIA.

34.4. Save as set out above, paragraph 34 is denied.

35. As to paragraph 35:

35.1. It is denied that any of the Additional Defendants, Mr del Rosso or Mr Grayson (or their respective companies) was a servant of RAKIA at any time.

35.2. It is admitted that, at the relevant time, Dechert was engaged by

RAKIA to provide legal advice and assistance pursuant to the Dechert Retainer. It is admitted that Dechert and Mr Gerrard were RAKIA's agents insofar as they performed that engagement on the instructions of RAKIA within the scope of the Dechert Retainer. If and insofar as Dechert or Mr Gerrard did any acts outside the scope of such instructions, such acts were not done with the authority or at the instigation of RAKIA, nor were they ratified by RAKIA.

35.3. It is admitted that at the relevant times Mr Buchanan was an agent of RAKIA.

35.4. It is denied that Mr Page (or his company) were agents of RAKIA.

35.5. It is denied that Mr del Rosso (or his company) were agents of RAKIA.

35.6. It is denied that Mr Grayson (or his company) were agents of RAKIA.

35.7. As to paragraph 35a.:

(a) It is admitted that, insofar as he was acting as the directing mind and will of RAKIA, Mr Buchanan's knowledge and conduct was attributable to RAKIA.

(b) It is further admitted that RAKIA is vicariously liable for Mr Buchanan's conduct while he was acting within the scope his authority.

(c) It is admitted that RAKIA is vicariously liable for Mr Gerrard's conduct while he was acting on the instructions of RAKIA within the scope of the Dechert Retainer.

35.8. As to subparagraph 35b.:

(a) It is alleged that RAKIA "*ratified*" unspecified "*acts or omissions*". It is assumed that this is intended to refer to alleged ratification of acts or omissions which were outside the scope of the authority of the relevant agent. If (which is not admitted) any of RAKIA's agents committed any acts or omissions which were outside the scope of their authority, then it is denied that RAKIA ratified such acts or omissions.

(b) It is denied that the Ruler ratified any unlawful acts or omissions of any of RAKIA's agents.

(c) It is denied that the Ruler was the *de facto* or *de jure* owner of RAKIA. RAKIA is and was at all relevant times owned by the Government of RAK.

- (d) It is denied that the Ruler was a *de facto* or *de jure* director of RAKIA. RAKIA has a Board of Directors which, at the relevant times, did not include the Ruler.
- (e) It is denied that Mr Buchanan ratified any unlawful acts allegedly committed by any of RAKIA's agents.
- (f) If (which is not admitted) Mr Gerrard had purported to ratify any unlawful acts allegedly committed by any of RAKIA's agents, such purported ratification would be outside the scope of the authority conferred upon Dechert and Mr Gerrard under the Dechert Retainer and therefore would not constitute a ratification by or on behalf of RAKIA.

35.9. As to paragraph 35c.:

- (a) It is admitted that RAKIA was vicariously liable for the acts and omissions of Dechert, Mr Gerrard and Mr Buchanan while they were acting within the scope of their respective authorities to act on RAKIA's behalf.
- (b) It is denied that RAKIA is vicariously liable for the acts or omissions of Mr Page, Mr del Rosso or Mr Grayson (or their companies) who were not its agents. Accordingly, if (which is not admitted) Mr Page, Mr del Rosso or Mr Grayson (or their companies) engaged in any such unlawful acts or omissions, those acts or omissions were neither authorised, instigated nor ratified by RAKIA and RAKIA is not vicariously liable in respect of them.

35.10. With the exception of the above, paragraph 35 is denied.

1. MR PAGE

36. As to paragraph 36:

36.1. It is denied that Mr Page was engaged by RAKIA. His engagement was on behalf of the Ruler and the Government of RAK to perform investigatory and related work relating, inter alia, to Dr Massaad and his associates. Pursuant to that engagement, Mr Page provided briefings and reports approximately once a month. Mr Page was not appointed as an agent of the Ruler, the Government of RAK or any other RAK entity but was, at all relevant times, an independent

contractor.

- 36.2. With the exception of the above, subparagraphs a. and b. are denied.
 - 36.3. As to subparagraph c., it is admitted that pursuant to an agreed security protocol, following Mr Page's briefings the hard copy of any written report discussed at the briefing was intended to be returned to Mr Page, with the intention that Mr Page would dispose securely of it. This arrangement was intended to ensure that the confidential contents of the reports remained secure and protected against unauthorised access by third parties. It is denied (if it is alleged) that there was anything improper about this arrangement.
 - 36.4. As to subparagraph d., it is admitted that Mr Page received very substantial remuneration of at least \$100,000 a month for his services. It is denied that the amount of Mr Page's remuneration supports any inference that the services he provided were risky.
 - 36.5. With the exception of the above, paragraph 36 is denied.
37. As to paragraph 37:
- 37.1. Subparagraphs a. and c. are admitted. In none of the cases referred to in those subparagraphs was Mr Page found by the court to have engaged in hacking or to have otherwise sought to obtain access to information unlawfully.
 - 37.2. As to subparagraph d., it is admitted that in *Re AI M* [2019] EWHC 3415 (Fam) the Family Division of the High Court made findings relating to Mr Page in the context of family law proceedings in which Mr Page was neither a party nor a witness and which did not concern any matters or allegations relating to RAKIA or the Government or Ruler of RAK. The court did not make any findings that Mr Page's conduct was criminal.
 - 37.3. With the exception of the above, paragraph 37 is not admitted.
38. The Re-Amended Counterclaim has abandoned, without explanation, the contention previously advanced at paragraph 38 of the Amended Counterclaim.
39. The inferential averments in paragraph 39 are outside RAKIA's knowledge

and are therefore not admitted.

2. MR DEL ROSSO

40. As to paragraph 40:

40.1. As to subparagraph a., it is admitted that Mr del Rosso engaged CyberRoot to provide services for RAK DEV. Paragraph 20.4 above is repeated. It is denied that the cost of those services indicates that the services were “*risky*” or “*very*” substantial.

40.2. Subparagraph aa. is denied.

40.3. As to subparagraph b., it is admitted that Mr del Rosso acted on the instructions of RAK DEV in arranging for the download of the hacked data from the Torrents.

40.4. With the exception of the above, paragraph 40 is denied.

41. Paragraph 41 is admitted.

C. THE PROJECT UPDATE

42. As paragraph 42:

42.1. In around January 2015, Mr Page was engaged by the Ruler to assist in asset tracing and recovery in respect of Dr Massaad.

42.2. In the course of that investigation (which was not targeted at Mr Azima) Mr Page received intelligence that Mr Azima was involved with Dr Massaad and others in organising a campaign to spread allegations against RAK.

42.3. By early 2015 RAKIA had not used any investigators to gather information on Mr Azima or others working with him (except in relation to Dr Massaad, whose substantial frauds and wrongdoing were the subject of various investigations).

42.4. With the exception of the above, paragraph 42 is denied.

43. As to paragraph 43:

43.1. It is admitted that on or after the date shown on the Project Update (26 March 2015) Mr Page provided the Project Update to Mr Buchanan. It is not admitted that Mr Page provided a copy of the Project Update to Mr Gerrard.

- 43.2. It is denied that Mr Page briefed the Ruler on the contents of the Project Update.
44. Save that the document destruction policy was Mr Page's and the redactions were to remove material irrelevant to this case, paragraph 44 is admitted.
45. Save that it is denied that Mr Cooper and Mr Behre were "*later also targeted*", paragraph 45 is admitted as a summary of the relevant passages of the "Project Update" document.
46. As to paragraph 46:
- 46.1. In Mr Page's witness statement he stated that "*my briefings to clients are invariably oral*" and that the first time he recalled hearing Mr Azima's name was in early 2016. In his oral evidence Mr Page accepted that he was aware of Mr Azima's name in 2015. Mr Page also explained that he regularly provided the Ruler with written update reports to accompany his oral briefings and he therefore accepted that the reference to briefings being "*invariably oral*" was therefore inaccurate. It is not admitted that Mr Page's evidence in his witness statement was dishonest.
- 46.2. It is admitted that Mr Page's witness statement did not contain the information described at subparagraphs b. i. to iv.. It is not admitted that Mr Page intentionally concealed that information.
47. As to paragraph 47:
- 47.1. It is admitted that witness statements for the First Trial were provided by (amongst others) Mr Gerrard (two), Mr Buchanan (four) and the Ruler (one).
- 47.2. It is admitted that Mr Gerrard did not refer to the Project Update in his witness statements. It is denied that Mr Gerrard suggested that he had first encountered Mr Page in August 2016. In his first statement, Mr Gerrard stated that he was first engaged by RAK in 2014 and that: "*At some stage in my relationship with RAK I was introduced to Stuart Page*".
- 47.3. Subparagraph b. is admitted. Although Mr Buchanan's witness

statement did not refer expressly to Mr Buchanan's dealings with Mr Page in 2015, Mr Buchanan explained that he "*met with Mr Page every month or so*" and provided details of one such meeting in February or March 2016. Mr Buchanan's witness statement did not conceal or attempt to conceal the contact between Mr Buchanan and Mr Page in 2015 nor were the contents of the statement in any way inconsistent with the existence of that contact.

47.4. It is admitted that the Ruler's witness statement did not refer to Mr Page. It is denied that the Ruler's witness statement suggested he was unaware of the Project Update or its contents. In his witness statement the Ruler stated that he had never seen the Project Update and Mr Azima was incorrect to suggest otherwise. The Ruler's statement that he had never seen the Project Update was true.

48. As to paragraph 48:

48.1. It is denied that Mr Buchanan and the Ruler intentionally concealed the true facts about the Project Update and Mr Page's reporting.

48.2. It is denied that RAKIA intended to procure the obtaining of any confidential information about Mr Azima, either through hacking or otherwise. Subparagraph b. is otherwise not admitted.

48.3. Subparagraph c. refers to unspecified "*proposals*". It is denied that RAKIA endorsed any proposals for any of Mr Azima's confidential information to be obtained (either through hacking or otherwise). Subparagraph c. is otherwise not admitted.

48.4. With the exception of the above, paragraph 48 is not admitted.

D. THE RULER'S INSTRUCTIONS TO "TARGET" AND "GO AFTER" MR AZIMA

49. As to paragraph 49:

49.1. In April 2015 the Ruler suspected that Mr Azima may have been involved with Dr Massaad's extensive criminality, and, if he was, he wanted appropriate civil proceedings or criminal charges to be brought against Mr Azima.

49.2. Accordingly, in early April 2015 the Ruler expressed a wish to Mr Buchanan for Mr Azima to be targeted (in the sense of seeking and assessing any information as to Mr Azima's possible role in any

criminal activity and, if it appeared that he had been involved in such activity, pursuing appropriate civil proceedings or criminal charges against him in respect of this).

49.3. This expression of wishes by the Ruler was not an instruction to undertake particular actions but was, rather, a communication of his current thinking.

49.4. With the exception of the above, paragraph 49 is denied.

50. As to paragraph 50:

50.1. On 4 April 2015, Mr Buchanan discussed the Ruler's wish with Mr Amir Handjani (a US lawyer and director of RAK Petroleum plc) and Mr Naser Bustami (a member of the board of RAK DEV). Mr Bustami sent an email the same day proposing that he, Mr Handjani and Mr Buchanan "*hook up and coordinate our attack*".

50.2. Mr Handjani, in turn, advised the Ruler against seeking to pursue charges against Mr Azima at that time, since doing so would be likely to disrupt attempts to engage with Dr Massaad through his lawyer. On 6 April 2015, Mr Handjani informed Mr Bustami and Mr Buchanan of this advice.

51. As to paragraph 51:

51.1. On 19 July 2015, Mr Buchanan sent an email to Mr Handjani in which he explained that Mr Bustami had informed him that the Ruler "*wants criminal stuff taken out of letter and to go after FA*". The reference to "*go[ing] after FA*" was a reference to the prospect of pursuing some form of civil proceedings or criminal charges against Mr Azima.

51.2. This was, again, not an instruction but rather an expression of the Ruler's current thinking.

51.3. With the exception of the above, paragraph 51 is denied.

52. As to paragraph 52:

52.1. As pleaded at paragraphs 49 to 51 above, the Ruler did not give any instructions to Mr Buchanan or Mr Bustami.

52.2. It is specifically denied that the statements by the Ruler pleaded at paragraphs 49 to 51 were acted upon by RAKIA's agents/alleged

agents taking steps to procure the hacking of Mr Azima's data.

52.3. For these reasons, paragraph 52 is denied.

E. MALICIOUS EMAILS RECEIVED BY MR AZIMA AND OTHERS

53. Paragraph 53 is admitted as a general description of the concepts of "*phishing*" and "*spear-phishing*".

54. As to paragraph 54:

54.1. It is admitted that on various dates in 2015 and 2016 a number of apparently suspicious emails (which included phishing and spear-phishing emails) were sent to Mr Azima and several other persons who were associated with him and/or Dr Massaad.

54.2. The emails listed in Schedule A are admitted.

55. As to paragraph 55:

55.1. It is denied that the content, timing, provenance and other characteristics of these emails indicate that they were sent as part of a single campaign targeting the recipients.

55.2. The majority of the emails listed in Schedule A appear to be common generic phishing or spam emails, which are likely to have been sent to many other individuals with no association with Dr Massaad or Mr Azima.

55.3. As to the remainder of paragraph 55:

(a) Subparagraph a. is admitted. It is denied that the five emails indicate that other emails in Schedule A were sent as part of a single campaign targeting the recipients.

(b) As to subparagraph b.:

(i) It is admitted that on 11 occasions substantively identical messages were sent to two recipients (Dr Massaad and Mr Cooper) at similar times from the same email address. Most of those 11 pairs of emails were sent from different email addresses.

(ii) The 11 pairs of emails sent to Dr Massaad and Mr Cooper appear to be generic phishing emails which did not contain any content specifically targeted at

Dr Massaad and Mr Cooper. There is nothing to indicate that any of those emails was specifically targeted at Dr Massaad and Mr Cooper or that they were sent by the same person or group of persons.

- (iii) Save as set out above, there are no other examples in Schedule A of substantively identical emails being sent from the same email address to more than one of the individuals listed in Schedule A.

55.4. As to subparagraph c., Mr Azima received a number of phishing emails including emails purporting to be from family members or business associates, an email purporting to be from Ms Beudjekian, and generic phishing emails which were not tailored to Mr Azima in any way.

55.5. Subparagraph d. is admitted. Mr Behre also received generic phishing emails which were not tailored to him in any way.

55.6. As to subparagraph e., Mr Behre received two emails at 6:26am and 6:42am on 26 March 2015 and several further emails between 27 March and 2 April 2015. It is denied that there is any connection between the Project Update and the sending of those messages.

55.7. As to subparagraph f., it is admitted that Mr Azima received a single email on 7 April 2015 and four emails on 10 April 2015. It is denied that there was any connection between those emails and the Ruler's alleged "instruction" to target Mr Azima.

55.8. As to subparagraph g.:

- (a) It is admitted that Mr Azima received emails listed in Schedule A on 7, 18 and 20 August 2015. It is not admitted (if it is alleged) that those emails were all spear-phishing emails.
- (b) It is not admitted (if it is alleged) that Mr Azima received any other phishing or spear-phishing emails in August 2015.
- (c) Further and in any event, it is denied that there was any connection between the Ruler's expression of his wish (reflected in an email sent by Mr Buchanan on 19 July 2015) to "*go after*" Mr Azima and Mr Azima's receipt of particular emails several weeks later in August 2015.

55.9. Paragraph h. is admitted. Mr Cooper received 47 emails listed in

Schedule A in April and May 2015. Many of those emails appear to be generic spam or phishing emails which were not tailored to Mr Cooper in any way.

55.10. As to subparagraph i., it is admitted that a small number of emails with false news regarding Mr Azima and Dr Massaad and their business operations were sent.

55.11. Subparagraph j. is not admitted.

55.12. As to subparagraph k.:

(a) The Re-Amended Counterclaim does not specify the “*technical characteristics*” referred to; nor does it identify which of the emails are said to possess those unspecified “*technical characteristics*”. If it is alleged that the presence of MESVR, “DidTheyReadIt?” and/or “Emkei” features in particular emails indicate that these emails were sent as part of a single campaign targeted at Mr Azima and his associates, this allegation is denied. In support of this denial:

- (i) MESVR is a very common tool used by attackers to mask the true sender of an email. Its use is not indicative that emails containing this feature were sent by a single attacker or group of hackers.
- (ii) DidTheyReadIt? is a standard tool which is commonly used for legitimate purposes and is unlikely to be used by proficient or sophisticated hackers.
- (iii) Emkei is a commonly used tool for sending spoof or anonymised emails. Of the emails which were apparently sent by the Emkei service, the majority were generic spam emails which were not specifically tailored or aimed at particular individuals.
- (iv) Accordingly, the fact that one or more of these features were present in a number of suspicious emails does not indicate that those emails were sent by the same attacker or group of attackers.

55.13. Except as set out above, paragraph 55 is not admitted.

56. Paragraph 56 is denied. RAKIA did not instruct anyone (whether directly or

indirectly) to send any phishing or spear-phishing emails. If (which is not admitted) any of the other Additional Defendants gave instructions to send any of the emails in Schedule A, this was done without the knowledge or authority of RAKIA and was not ratified by RAKIA.

F. SUSPICIOUS ACCESS TO CERTAIN EMAIL ACCOUNTS

57. The matters pleaded in paragraph 57 are outside RAKIA's knowledge and are therefore not admitted.

G. THE "VIEW FROM THE WINDOW" DOCUMENT

58. As to paragraph 58:
- 58.1. The "View from the Window" document was prepared by Karv Communications which was not a consultant to RAKIA. Paragraph 32.2(c) above is repeated.
- 58.2. With the exception of the above, paragraph 58 is admitted. RAKIA will refer to the document at trial for its full terms.
59. As to paragraph 59:
- 59.1. It is denied that Mr Buchanan was "*leading the RAK Project*". There was no such project. Mr Buchanan was leading the investigations into Dr Massaad and the persons associated with him.
- 59.2. Subparagraph b. is admitted.
60. As to paragraph 60:
- 60.1. The "View from the Window" document was written by Mr Frank. It was not written by RAKIA, Mr Buchanan or Mr Gerrard and therefore no inference can be drawn from any alleged omission by RAKIA, Mr Buchanan or Mr Gerrard to explain the basis or intended meaning of particular words used by Mr Frank in that document.
- 60.2. In any event, as is apparent from the form and content of the "View from the Window" document, it consisted of draft and self-evidently incomplete notes written in rough bullet-point form by a public relations adviser. It was not (and did not purport to be) an account of findings reached by an investigator. The expression "*exposed as fact*" in the document must be read and understood in this context. Further:

- (a) The expression “*exposed as fact*” appears in the eighth line of the document and was not linked specifically or exclusively to the reference to Mr Azima contained in the fifteenth and sixteenth lines of the document.
- (b) The suggestion that the expression “*exposed as fact*” must be read literally is untenable in circumstances where some of the matters to which that expression relates were themselves expressed in qualified or tentative terms which are inconsistent with a statement of unqualified fact (for example, the statement that Mr Azima “*appears to have orchestrated...fraudulent activities*” and the reference to “*Possible gun running, drug transport, plane sales*”).

61. The inference pleaded at paragraph 61 is denied. In support of this denial, RAKIA will rely on the following matters:

61.1. At the time when the “View from the Window” document was produced by Mr Frank on 29 December 2015:

- (a) The negotiations between Mr Azima and RAKIA regarding the settlement of Mr Azima and HeavyLift’s claims concerning the RAK-HeavyLift Training Academy joint venture were ongoing. RAKIA’s entry into the Settlement Agreement (which was a consequence of Mr Azima’s fraudulent misrepresentations) did not occur until more than two months later.
- (b) The negotiations between RAKIA and Mr Azima concerning the Proposed ISR Joint Venture had barely begun. In particular:
 - (i) Four of the five alleged false representations made by Mr Azima regarding the Proposed ISR Joint Venture were not made until late January or February 2016 (i.e. several weeks after the date of the “View from the Window” document).
 - (ii) The fifth false representation was made in a document sent to Mr Buchanan on the evening of 28 December 2015 (i.e. just one day before the “View from the Window” document was produced). The emails from Mr Adams and Mr Lepper which demonstrated the falsity of that

representation were not written and sent until at least several weeks later.

Accordingly, as at the date of the “View from the Window” document, RAKIA did not have any potential claim for fraudulent misrepresentation against Mr Azima and it could not have known that Mr Azima had committed “*numerous frauds*” against it.

61.2. Further, RAKIA’s lack of knowledge in late 2015 regarding (1) Mr Azima’s frauds and wrongdoing in relation to the Sham Referral Agreement, (2) Mr Azima’s false claim to have introduced the prospective purchasers of the Hotel to RAKIA, (3) the falsity of the HeavyLift Investment Misrepresentation, and (4) Mr Azima’s role in relation to the production of the “Security Assessment”, is reflected by the fact that RAKIA’s original pleaded case served on 30 September 2016 did not contain any allegations or claims regarding these matters. Instead:

- (a) RAKIA’s claims and allegations based on the Sham Referral Agreement and Mr Azima’s false representation that he had introduced the prospective purchasers of the Hotel to RAKIA, were not advanced until shortly before RAKIA served its Amended Particulars of Claim on 11 December 2017.
- (b) RAKIA’s claims and allegations concerning the HeavyLift Investment Misrepresentation and the “Security Assessment” were not advanced until shortly before RAKIA served its Re-Amended Particulars of Claim on 19 July 2018.

H. THE RULER’S “WIDER OBJECTIVES”

62. Paragraph 62 is admitted.

63. As to paragraph 63:

63.1. The Settlement Agreement was negotiated and drafted by Dechert (representing RAKIA) and Miller & Chevalier (representing Mr Azima and HeavyLift) over a period of several weeks in late 2015 and early 2016. During the course of the negotiations regarding the terms of the agreement, Dechert and Miller & Chevalier both made a number of revisions to the draft terms and text of the Settlement Agreement.

63.2. Paragraph 63 is otherwise admitted.

64. Paragraph 64 is admitted. RAKIA will refer to the letter of recommendation at trial for its full terms.

65. As to paragraph 65:

65.1. The inferences pleaded are an impermissible attempt to reopen matters which are the subject of factual findings in the Judgment which the Court of Appeal has held are final and incapable of being reopened in the trial of the Counterclaim. Paragraph 65 is therefore liable to be struck out.

65.2. Without prejudice to this contention, paragraph 65 is denied in that:

- (a) The expression “*wider objectives*” in the letter seeking the Ruler’s approval of the Settlement Agreement was a reference to the aims of (1) resolving other potential claims and (2) attempting to reach a settlement with Dr Massaad. The latter aim was expressly reflected in Recital (E) to the Settlement Agreement, which stated that: “*Mr. Azima has recently provided negotiation assistance to RAKIA on an informal basis which RAKIA recognises and appreciates*”.
- (b) The purposes of the good faith clause in the Settlement Agreement were:
 - (i) to provide RAKIA with an assurance that Mr Azima’s representations regarding the value of HeavyLift’s contribution to the Training Academy Joint Venture were correct, in circumstances where RAKIA was unable to verify independently what, if anything, was properly owed to HeavyLift;
 - (ii) to provide RAKIA with an assurance that Mr Azima was acting (and would continue to act) in good faith in the context of the ongoing sensitive discussions between RAKIA’s lawyers and Mr Azima concerning matters relating to Dr Massaad; and
 - (iii) to reflect the fact that RAKIA’s entry into the Settlement Agreement was premised on what RAKIA regarded as a

moral obligation to Mr Azima, rather than a legal obligation, and it was therefore appropriate for the payment of \$2.6 million to Mr Azima pursuant to that moral obligation to be accompanied by an assurance as to the probity and integrity of Mr Azima's conduct towards RAKIA and its related entities.

- (c) Had RAKIA wished to make damaging allegations against Mr Azima which would attract significant publicity, it could have achieved that objective without having to engage in a convoluted process of negotiating and drafting a Settlement Agreement incorporating a good faith clause, paying Mr Azima \$2.6 million pursuant to that Settlement Agreement, and then embarking upon protracted and costly legal proceedings in order to recoup those monies. In particular:
 - (i) RAKIA could have publicised Mr Azima's wrongdoing and made damaging allegations about his conduct without having to resort to legal proceedings at all.
 - (ii) If (which is denied) RAKIA had been aware in early 2016 of Mr Azima's frauds concerning the Sham Referral Agreement and the false representation that he introduced the buyers of the Hotel to RAKIA, then RAKIA could have issued proceedings for unlawful means conspiracy against Mr Azima in respect of this wrongdoing. RAKIA's ability to bring such a claim was in no way dependent upon the existence of the good faith clause.
- (d) Further, if RAKIA had intended to use the Settlement Agreement as a vehicle for causing serious damage to Mr Azima's reputation, then it would have been illogical for RAKIA to agree to the inclusion in the Settlement Agreement of:
 - (i) a recital which recorded that: *"Each Party has the greatest of respect for the other Parties"*;
 - (ii) a recital which recorded RAKIA's *"recogni[tion] and appreciate[ion]"* for Mr Azima's assistance in

negotiations; and

- (iii) an express “*NON-DISPARAGEMENT*” clause, which provided that: “*Each Party agrees not to disparage any other Party... In particular, the Parties shall not at any time publish or otherwise make any statement concerning any other Party...which is derogatory or disparaging or which is intended or could reasonably be expected to lower their respective reputations.*”

65.3. It is specifically denied that at the date when the Settlement Agreement was drafted and entered into RAKIA had accessed and analysed data from Mr Azima’s computers and emails. Paragraph 61 above is repeated.

I. THE MEETING OF 16 JULY 2016

66. As to paragraph 66:

66.1. It is admitted that, on 16 July 2016, a meeting was held between Mr Azima, Mr Buchanan, Mr Gerrard, and a Dechert associate (“the **16 July Meeting**”).

66.2. This was a without prejudice meeting. In his Re-Re-Amended Defence to RAKIA’s claims, Mr Azima disregarded the without prejudice status of the 16 July Meeting by pleading allegations about what was said at that meeting. In a judgment dated 19 November 2019, HHJ McCahill QC held that since the 16 July Meeting had taken place on a without prejudice basis, the contents of the meeting should not have been referred to in Mr Azima’s statement of case, but that since Mr Azima had disregarded this RAKIA was entitled to respond to those allegations in its Re-Amended Reply. RAKIA responds to the allegations about the 16 July Meeting at paragraphs 66 and 67 of the Re-Amended Counterclaim on the same basis and without this response entailing any waiver or loss of the without prejudice privilege status of the contents of that meeting.

66.3. As to the matters at subparagraphs a. to c.:

- (a) Subparagraph a. is admitted. Mr Gerrard had previously asked Mr Azima about whether he had always acted in the interests of the Ruler and referred to issues concerning HeavyLift and

Eurasia Hotel Holdings Limited ("**Eurasia**"). Those questions arose from:

- (i) The publication of the so-called "Panama Papers" (a leak of documents from the Panamanian law firm Mossack Fonseca) in around April 2016, which contained documents that raised questions about the nature of Mr Azima's interest in Eurasia; and
 - (ii) An investigation by Dechert in 2016 into complex and unusual transactions involving changes in the ownership of HeavyLift, which had at various times in the past been partly owned by various RAK entities before Mr Azima became the sole shareholder.
- (b) As to subparagraph b.:
 - (i) It is admitted that Mr Gerrard's questions to Mr Azima indicated that he had concerns about the conduct of HeavyLift and Eurasia. No admissions are made regarding Mr Gerrard's state of knowledge regarding this. It is denied (if it is alleged) that Mr Gerrard asked questions to Mr Azima in Mr Buchanan's presence which indicated that Mr Gerrard believed that Mr Azima had engaged in any of the fraudulent activities which subsequently formed the subject of RAKIA's claims against Mr Azima.
 - (ii) The fact that Mr Gerrard asked questions which reflected the existence of concerns on his part about the conduct of HeavyLift and Eurasia is not inconsistent with Mr Buchanan having only believed that Mr Azima had engaged in fraudulent activities and wrongdoing after RAKIA obtained and analysed the hacked data following its publication on the internet in August and September 2016.
- (c) Subparagraph c. is denied. In particular:
 - (i) Mr Gerrard did not want, nor did he request or seek to persuade, Mr Azima to change his allegiance from Dr Massaad to RAKIA. Such a change of allegiance

would have been counterproductive and contrary to RAKIA's interests in the negotiations, since communicating with Dr Massaad was already very difficult and it was likely that Dr Massaad would disengage from the negotiations altogether if he had reason to believe that Mr Azima had taken RAKIA's side in the negotiations.

- (ii) During the 16 July Meeting Mr Gerrard reported that Mr Kirby Behre (who was counsel to both Dr Massaad and Mr Azima) had suggested that civil and criminal claims against Dr Massaad would result in "*mutually assured destruction*". Mr Gerrard went on to say that the further the matter went, the more likely it was that collateral damage would occur because it would be difficult to keep the scope of RAKIA's actions within a narrow compass. There was no suggestion or threat that damage would be caused to Mr Azima.

67. Paragraph 67 is denied insofar as it relates to the knowledge and expectations of RAKIA and is otherwise not admitted.

J. THE EMAILS "BREAKING THE NEWS"

68. Paragraph 68 is admitted.

69. Paragraph 69 is admitted.

70. Paragraph 70 is admitted.

71. As to paragraph 71:

71.1. It is denied that the emails referred to at paragraphs 68 to 70 were written to confect a documentary trail purporting to evidence the "innocent discovery" of the Torrents as alleged or at all.

71.2. The contention that those emails were sent for the purpose of creating a false narrative that RAKIA first learned of the websites on 15/16 August 2016 is inconsistent with the fact neither RAKIA nor any of its

witnesses ever sought to advance any such narrative (either by reference to those emails or otherwise). On the contrary:

- (a) In its Part 18 response dated 6 November 2018, RAKIA stated that Mr Buchanan had first become aware of the publicly available links “*in the first week of August 2016*”.
- (b) As pleaded at paragraph 71a.i.-ii. of the Re-Amended Counterclaim, RAKIA’s evidence at trial was that:
 - (i) Mr Gerrard had discussed the websites with Mr Buchanan and Mr del Rosso on 8 or 9 August 2016; and
 - (ii) Mr del Rosso, on Mr Gerrard’s instruction, engaged NTi to begin downloading the hacked data on 12 August 2016.
- (c) In his first witness statement, Mr Buchanan admitted that the reference (in the email described at paragraph 70 of the Re-Amended Counterclaim) to Mr Page having informed Mr Buchanan “*last night*” was inconsistent with the fact that Mr Buchanan had initially been informed of the existence of the first tranche of the hacked data approximately a week or so earlier. If Mr Buchanan had been deliberately seeking to fabricate a documentary trail to support a false account about when and how he had learned of the hacked data, he would not have included a statement in that fabricated documentary trail which was inconsistent with the false account he was seeking to support.

71.3. Further, three of the emails sent by Mr Gerrard, Mr del Rosso and Mr Buchanan on 15/16 August 2016 contained references to the website having been “*set up*”, “*emanat[ing]*” and “*based*” in the “*UAE*”. If Mr Gerrard, Mr del Rosso and Mr Buchanan were seeking to create a false documentary trail to divert suspicion from themselves and RAKIA, then it would be illogical for them to refer to the website in question being established in, emanating from and/or based in the UAE.

71.4. As to the specific matters pleaded at paragraph 71a. i.-vii.:

- (a) Subparagraphs i.-ii. are admitted. Paragraph 71.2 of this

Defence to the Re-Amended Counterclaim is repeated.

- (b) Subparagraph iii. is admitted.
- (c) Subparagraph iv. is not admitted.
- (d) Subparagraph v. is admitted.
- (e) Subparagraph vi. is not admitted.
- (f) Subparagraph vii. is admitted.

71.5. Paragraph 71b. is denied.

K. THE TORRENTS

72. Save that it is not admitted that the hacked data contained information which was private, confidential or privileged, paragraph 72 is admitted.

73. As to paragraph 73:

73.1. It is admitted that the hacked data was apparently obtained without Mr Azima's authorisation and included emails from the 10 email accounts listed at subparagraph b. and the types of data listed in subparagraph c.

73.2. RAKIA does not know the precise numbers of emails, photographs/images and voice recordings contained in the hacked data. Subparagraph d is therefore not admitted.

73.3. Subparagraph e. is not admitted.

74. As to paragraph 74:

74.1. In relation to subparagraphs a.-c.:

(a) It is admitted that in August and September 2016 RAKIA acquired (through NTi and Vital) copies of the hacked data from the internet where the hacked data was publicly available via the Torrents. RAKIA thereafter analysed the hacked data for the purpose of investigating and establishing the extent of Mr Azima's frauds.

(b) It is denied that RAKIA was responsible for the hacking or publication of the hacked data on the Torrents. RAKIA does not know who was responsible for this.

74.2. As to subparagraph d., it is admitted that on 23 September 2016 Dechert sent a pre-action letter to Mr Azima's US lawyers, Miller &

Chevalier, which referred to documents obtained from the hacked data and enclosed copies of some of those documents. It is denied that any of those documents (which contained evidence of Mr Azima's frauds and which had been obtained from the publicly available Torrents) were confidential. Paragraph 6.3 above is repeated.

74.3. Subparagraphs e. and f. are admitted.

75. As to paragraph 75:

75.1. Subparagraph a. is admitted.

75.2. Save that it is denied that RAKIA "*changed*" its case regarding how it learned of and obtained the hacked data, subparagraph b. is admitted. The reference to a public relations company in Mr Hughes' witness statement dated 13 July 2018 was intended to be a reference to Mr Page and his company, Stuart Page MEFZ. Mr Page and Stuart Page MEFZ were erroneously described as a "*public relations company*". The explanation contained in Mr Hughes' witness statement and in RAKIA's further information dated 6 November and 11 December 2018 accurately described both:

- (a) the identity of the person (Mr Page) who first informed RAKIA of the existence of publicly available links to the first and second Torrents containing links to the hacked data; and
- (b) what RAKIA was told by Mr Page about how he had learned of those publicly available links.

76. As to paragraph 76:

76.1. It is denied that RAKIA's account of how it obtained the hacked data was not supported by any documentary evidence. RAKIA disclosed various contemporaneous emails sent to/from Mr Buchanan, Mr Gerrard, Mr del Rosso and two employees at NTi, Richard Garcia and Jessica Gray, in respect of the discovery and acquisition of the hacked data.

76.2. Save that it is assumed that the reference to an email sent by Mr del Rosso "*on 9 September 2016*" is a typographical error, and should read "*on 9 August 2016*", subparagraph a. is admitted.

76.3. Subparagraph b. is admitted.

76.4. As to subparagraph c.:

- (a) On 22 August 2016, Ms Gray informed Mr Garcia that because there was only one 'seeder' which held the relevant files she was encountering difficulty in downloading that file, but that she would attempt various means to overcome this issue.
- (b) On 23 August 2016, Mr Garcia informed Mr del Rosso about this difficulty but stated that some of the data in the files would be provided to Mr del Rosso the following day.
- (c) On 24 August 2016, Ms Gray informed Mr Garcia that she had successfully accessed and downloaded all of the files.

76.5. Subparagraph d. is denied:

- (a) It is common ground that NTi downloaded the hacked data in August and September 2016. This demonstrates that the hacked data was publicly accessible on the internet on those dates.
- (b) Mr Azima's advisers learned of the existence of the first Torrent in early August 2016 as a result of a "Google Alert" set up on Mr Azima's name. This demonstrates that that Torrent was publicly accessible and easily discoverable via public internet search engines at that time.
- (c) RAKIA's IT expert in the US Proceedings did not attempt to download the hacked data until between 31 March and 10 April 2017 (i.e. more than seven months after the hacked data first became available). The fact that RAKIA's expert was able to download some, but not all, of the hacked data in a ten-day period in March/April 2017 does not cast any light on the public accessibility of the hacked data in August/September 2016. In support of this contention RAKIA will rely inter alia on the joint expert report dated 28 November 2019 of the parties' forensic IT experts in these proceedings, Christopher Tarbell and Winston Krone, which confirms that the availability of data shared over a Torrent may change over time and that it is not possible to retrace peer-to-peer activity involving such Torrents.

77. As to paragraph 77:

77.1. It is denied that RAKIA presented a false case as to how it obtained the hacked data or as to its knowledge of who created the Torrents.

77.2. As pleaded at paragraph 74.1 above, in August and September 2016 RAKIA obtained, (though NTi and Vital) copies of the hacked data which was publicly available on the internet via Torrents. RAKIA did not and does not know who created the Torrents.

77.3. For these reasons, paragraph 77 is denied.

L. VITAL'S ALLEGED ENGAGEMENT OF 'HACK FOR HIRE' FIRMS

77A. As to paragraph 77A:

77A.1 It is denied that CyberRoot or Cyber Defence and Analytics hacked Mr Azima's data and devices on behalf of RAKIA as alleged at paragraph 77A.

77A.2 Paragraph 77A is otherwise not admitted.

77B. Paragraph 77B is not admitted.

1. CyberRoot

78. Paragraph 78 is admitted.

79. As to paragraph 79, the purpose of the payments made by Vital to CyberRoot is set out paragraph 20 above.

80. As to paragraph 80:

80.1. It is not admitted that Gravitas made payments to CyberRoot between 2015 and 2017.

80.2. If and insofar as such payments were made, it is denied that they were made on behalf of RAKIA.

81. As to paragraph 81:

81.1. It is not admitted that CyberRoot is a "*hack for hire*" firm. Paragraph 20 above is repeated.

81.2. It is denied that the CyberRoot hacked Mr Azima's emails and devices on behalf of RAKIA as alleged.

81.3. As to the matters relied on:

- (i) Subparagraph a. is not admitted.
- (ii) Subparagraph b. is admitted.
- (iii) The press report pleaded at subparagraph c. is admitted. No admissions are made regarding the accuracy of the contents of that press report.
- (iv) Subparagraphs d. and e. are not admitted.
- (v) As to subparagraph f., no admissions are made regarding the contents or accuracy of any statements alleged to have been made by Mr Pandey to Mr Rey. Paragraph 22 above is repeated.
- (vi) Subparagraph g. is not admitted.
- (vii) Subparagraph h. is denied. Paragraph 79 above is repeated.
- (viii) Subparagraph i. is not admitted. Paragraph 80 above is repeated.

2. Cyber Defence and Analytics

81A. Paragraph 81A is not admitted.

81B. As to paragraph 81B:

81B.1 It is denied that Cyber Defence and Analytics hacked Mr Azima's data and devices on behalf of RAKIA as alleged.

81B.2 As to the matters relied on:

- (a) It is denied that Vital was instructed to carry out work for RAKIA at any relevant time. It is further denied (if it is alleged) that Vital provided instructions to Cyber Defence and Analytics for or on behalf of RAKIA.
- (b) Subparagraph a. is otherwise not admitted.
- (c) Subparagraph b. is not admitted.
- (d) Subparagraph c. is not admitted.
- (e) Subparagraph d. is not admitted.
- (f) Subparagraph e. is not admitted.
- (g) Save that it is admitted that documents purporting to be bank statements purportedly show that Vital made payments of \$17,480 and \$4,000 to Cyber Defence and Analytics on 3 and

27 June 2016 respectively, subparagraph f. is not admitted.

81C. Save that it is admitted that Mr del Rosso and Mr Jain communicated via messages in 2020, the unparticularised allegations at paragraph 81C are not admitted.

M. THE DELETION OF MR BUCHANAN'S EMAILS

82. Paragraphs 82 to 87 of the Re-Amended Counterclaim contain various allegations concerning the deletion of emails from Mr Buchanan's MSN email account in October 2016 ("the **Email Deletion Issue**") and the truth of Mr Buchanan's evidence at the First Trial regarding this. As to this:

82.1. Mr Buchanan provided a total of four witness statements at the First Trial including one witness statement which contained a detailed account of the circumstances in which his emails were deleted by an employee at the Apple Store in Covent Garden, London and the extensive steps that Mr Buchanan subsequently took (with expert assistance from cyber specialists at Control Risks) to restore emails which had been deleted by the Apple Store employee.

82.2. During the course of Mr Buchanan's cross-examination (which lasted three days) Mr Buchanan was questioned and challenged extensively regarding the circumstances of the email deletion and the truthfulness of his evidence regarding this. On the basis of his assessment of all of the relevant documentary and oral evidence, the Judge:

- (a) found that Mr Buchanan was "*a generally reliable witness who gave his evidence in a measured way and was prepared to concede a number of points adverse to RAKIA's case that were put to him in cross examination*"; and
- (b) in relation to the Email Deletion Issue, "*accept[ed] Mr Buchanan's evidence on this point and conclude[d] that he had not deliberately destroyed any emails*".

82.3. The Judge's findings that Mr Buchanan was a generally reliable witness and had not deliberately destroyed any emails are final and cannot be reopened or challenged in the context of the trial of the Counterclaim. The allegations concerning the Email Deletion Issue at paragraphs 81 to 86 of the Re-Amended Counterclaim are therefore

liable to be struck out on the basis that they are an impermissible attempt to reopen factual findings which the Court of Appeal has held are final and conclusive.

82.4. Further and in any event, the allegations concerning the Email Deletion Issue at paragraphs 81 to 86 are evidential matters which go solely to Mr Buchanan's credit. These paragraphs are therefore liable to be struck out on the basis that they are an impermissible attempt to plead evidence and/or matters going solely to credit. RAKIA pleads to these paragraphs without prejudice to this contention.

83. As to paragraph 82:

83.1. It is admitted Mr Buchanan was RAKIA's primary disclosure custodian for the purposes of its disclosure given in relation to Mr Azima's hacking allegations.

83.2. In addition to Mr Buchanan, RAKIA provided disclosure in relation to Mr Azima's hacking allegations from various other sources including from within RAK DEV and from third parties.

83.3. It is denied that Mr Buchanan was RAKIA's primary disclosure custodian in respect of other issues for which disclosure was given.

84. Paragraphs 83 and 84 are admitted. RAKIA's solicitors subsequently informed Mr Azima's solicitors that the date on which Mr Buchanan's emails had been deleted by the Apple store employee was 14 October 2016 and the reference to 12 October 2016 had been a typographical error.

85. As to paragraph 85:

85.1. It is admitted that of the 198 individual emails sent to Mr Azima by Mr Buchanan that were disclosed by Mr Azima, only one is available as an individual email on the images taken of Mr Buchanan's account. However, a number of the 198 individual emails are found in the images of Mr Buchanan's account as emails within email chains (for example where a reply was received by Mr Buchanan to emails sent by him).

85.2. It is admitted that of the 106 individual emails sent to Mr Buchanan that were disclosed by Mr Azima, 83 are found as individual emails on

the images taken of Mr Buchanan's account. Additional emails from the 106 individual emails sent by Mr Azima are found in the images of Mr Buchanan's account as emails within email chains.

85.3. With the exception of the above, paragraph 85 is denied.

86. Paragraph 86 is admitted. In his fourth witness statement dated 12 November 2019, Mr Buchanan provided a detailed account of the circumstances in which the emails were mistakenly deleted by an employee at the Apple Store in Covent Garden, London.

87. As to paragraph 87:

87.1. It is denied that Mr Buchanan's account was false. As the Judge rightly held, Mr Buchanan's account of the Email Deletion Issue is true and no emails were deliberately destroyed.

87.2. As to the remainder of the paragraph:

(a) Subparagraph a. is denied. The emails were deleted from Mr Buchanan's MSN email account by an Apple Store employee in the circumstances described in Mr Buchanan's fourth witness statement.

(b) As to subparagraph b.:

(i) In relation to the first sentence, Mr Buchanan's understanding was that the Apple Store employee deleted emails from the sent items and deleted items from folders of his MSN email account and that the deletion of emails from those folders would not have resulted in the loss of emails from the inbox or sub-folders of that email account. It is nevertheless possible that the Apple Store employee may also have deleted emails from the inbox and its subfolders. Enquiries undertaken on behalf of RAKIA have been unable to ascertain whether this did in fact occur.

(ii) The second sentence of subparagraph b. is not admitted.

(c) As to subparagraph c., it is admitted that Mr Buchanan did not inform RAKIA's solicitors, Stewarts Law LLP ("**Stewarts**") in August 2017 about the incident at the Apple Store. Shortly after

the Apple Store incident occurred, Mr Buchanan had informed RAKIA's then solicitors, Dechert, about the incident. Mr Buchanan then sought, with the assistance of cyber specialists at Control Risks, to ensure that relevant deleted emails were recovered. In December 2016, an independent IT company and disclosure provider, Millnet, was engaged to produce a forensic image of Mr Buchanan's MSN email account. Having informed RAKIA's solicitors about the Apple Store incident at the time of the incident, and believing that all relevant emails had been recovered with the assistance of Control Risks and then captured by the forensic image of his MSN Email Account produced by Millnet in December 2016, it did not occur to Mr Buchanan that there was any need in August 2017 to remind RAKIA's new solicitors about the Apple Store incident that had taken place some 10 months earlier.

- (d) Subparagraph d. is denied. RAKIA disclosed contemporaneous emails which referred to the deletion of Mr Buchanan's emails at the Apple Store:
 - (i) In an email to Mr Buchanan sent on 24 October 2016, a consultant at Control Risks, Joe Littledale, referred to *"your question regarding the recovery of the emails deleted...by the Apple Store employees"*.
 - (ii) In a further email to Mr Buchanan sent on 27 October 2016, Mr Littledale explained that *"we propose to reinstate all the emails from the month of October (thereby capturing any emails which may have been deleted erroneously by the Apple Store employees)"*.
- (d) As to subparagraph e., it is admitted that during his cross-examination Mr Buchanan stated that he had been accompanied to the Apple store by another person. Mr Buchanan was not asked to identify that person during his cross-examination.

N. MR GERRARD'S AND MR HUGHES' EVIDENCE AS TO DEALINGS WITH MR AL SADEQ

88. Paragraphs 88 to 95 contain various allegations about the accuracy of the evidence given by Mr Gerrard at and shortly after the First Trial regarding interviews he conducted with RAKIA's former general counsel, Karam Al Sadeq, and evidence given by Mr David Hughes in 2015 in *RAKIA v Bestfort Development LLP* ("the **Bestfort Proceedings**") regarding interviews he had conducted with Mr Al Sadeq. These allegations go solely to the credit of Mr Gerrard and Mr Hughes and are irrelevant to the issues that arise for determination in the Counterclaim. In particular:

88.1. In the Addendum to the Judgment dated 30 June 2020, the Judge expressly held that Mr Gerrard's evidence at the First Trial regarding his interviews of Mr Al Sadeq and the corrective evidence regarding this issue in Mr Gerrard's corrective witness statement were irrelevant to Mr Azima's hacking allegations. The accuracy of Mr Gerrard's evidence concerning his interviews of Mr Al Sadeq is therefore irrelevant to the issues that arise for determination in the Counterclaim.

88.2. Mr Hughes was not a witness of fact in the present proceedings and he is not alleged to have had any involvement in the hacking of Mr Azima's emails/devices. The Bestfort Proceedings took place in 2015 and concerned applications for freezing orders and the appointment of receivers over a number of English-registered limited liability partnerships alleged to be connected with a Georgian national named Gela Mikadze. The accuracy of a single sentence in one of Mr Hughes' witness statements in those proceedings is entirely irrelevant to the issues that arise for determination in the Counterclaim.

88.3. In correspondence with RAKIA's solicitors, Mr Azima's solicitors have sought to justify the inclusion of the allegations in paragraphs 88 to 95 of the Re-Amended Counterclaim on the basis that they provide evidential "*corroboration*" and "*confirmation*" that Mr Gerrard is not a credible witness and RAKIA is not a reliable party. It is impermissible to plead evidence in a statement of case in support of an assertion regarding the credibility of a witness or party.

88.4. It follows that paragraphs 88 to 95 of the Re-Amended Counterclaim are liable to be struck out. RAKIA's response to those paragraphs set

out below is without prejudice to RAKIA's primary position that paragraphs 88 to 95 are an impermissible pleading and should not form part of the Re-Amended Counterclaim at all.

89. Paragraph 88 is admitted. As to Mr Al-Sadeq:

89.1. He was convicted in 2015 and 2017 of defrauding RAKIA and other RAK entities and is currently serving a sentence of imprisonment in respect of those offences; and

89.2. He was found by the Judge in the present proceedings to have been a party to the unlawful conspiracy in which Mr Azima received illicit payments totalling \$1,652,500 and a bribe of \$500,000 was paid to Dr Massaad.

90. Paragraphs 89 and 90 are admitted.

91. It is admitted that Mr Gerrard gave evidence at the First Trial, summarised in paragraph 91. RAKIA will, if necessary, refer to the full transcript of Mr Gerrard's evidence.

92. It is admitted that following the handing down of the Judgment, Mr Gerrard provided a corrective witness statement, summarised in paragraph 92. RAKIA will, if necessary, refer to the full witness statement at trial.

93. Paragraph 93 is admitted

94. Paragraph 94 is not admitted.

95. As to paragraph 95:

95.1. The Bestfort Proceedings were not proceedings in which hacking was an issue. It was an application for freezing orders in support of foreign proceedings. RAKIA has been unable to identify the complaint of hacking referred to.

95.2. It is admitted that Mr Hughes represented RAKIA in the Bestfort Proceedings.

95.3. Subparagraphs a. and b. are admitted.

- 95.4. It is admitted that the evidence given by Mr Hughes was inaccurate. At the time he made the statement Mr Hughes understood that no interviews had taken place before October 2015.
- 95.5. It is denied that Mr Hughes gave false evidence in order to serve RAKIA's interests.
- 95.6. With the exception of the above, paragraph 95 is denied.

O. MR PAGE'S THREAT TO "IMPLICATE" OTHERS

96. Paragraph 96 is admitted.
97. Save that RAKIA does not plead to the comment in the second sentence, paragraph 97 is admitted.
98. Paragraph 98 is denied insofar as it relates to the Ruler's alleged involvement in wrongdoing and is otherwise not admitted.

P. FURTHER PUBLICATION ON WETRANSFER SITES

99. As to paragraph 99:
- 99.1. It is admitted that a large volume of data originating from Mr Azima's emails and/or computers was disseminated on WeTransfer sites.
- 99.2. It is admitted that one dataset was made available on WeTransfer on 3 June 2019. The continued availability of that dataset is not admitted.
- 99.3. With the exception of the above, paragraph 99 is not admitted.
100. As to paragraph 100:
- 100.1. No admissions are made regarding the truth of any statements or admissions allegedly made by Mr Pandey to Mr Rey. Paragraph 22 above is repeated.
- 100.2. It is not admitted that CyberRoot made data belonging to Mr Azima available on WeTransfer sites, and it is denied that RAKIA had any knowledge of or instructed or ratified any such action by any party.
- 100.3. With the exception of the above, paragraph 100 is not admitted.

IV. THE HACKING OF MR AZIMA AND THE COVER UP OF THE FACTS RELATING TO IT

101. RAKIA does not plead to paragraph 101 as it does not contain any averment of fact.
102. Save that it is admitted that an unknown person or persons obtained Mr Azima's emails, paragraph 102 is not admitted.
103. As to paragraph 103:
- 103.1. RAKIA does not know who was instructed to hack and disseminate Mr Azima's data or to procure others to do so.
 - 103.2. If and insofar as it is alleged that individuals authorised to act on behalf of RAKIA gave such instructions or procured others to do so on behalf of RAKIA, or that RAKIA subsequently ratified such instructions or procuring, this allegation is denied.
 - 103.3. Mr Page was not instructed or authorised by RAKIA to engage hackers to attack Mr Azima.
 - 103.4. Mr del Rosso and/or Vital were not instructed or authorised by RAKIA to engage CyberRoot or Cyber Defence and Analytics (or anyone else) to carry out hacking of Mr Azima or Dr Massaad or to disseminate Mr Azima's data.
 - 103.5. With the exception of the above, paragraph 103 is not admitted.
104. As to paragraph 104:
- 104.1. It is denied that Mr Page, Mr del Rosso or Vital were, at any time, agents of RAKIA and, as a result, it is denied that their knowledge and conduct is attributable to RAKIA.
 - 104.2. If and insofar as it is so alleged, it is denied that RAKIA instigated, authorised or ratified the alleged or any unlawful acts by Mr Page, Mr del Rosso or Vital.
 - 104.3. For these reasons, paragraph 104 is denied.
105. It is denied that Mr Buchanan paid CyberRoot for any services on behalf of RAKIA. RAKIA and Mr Buchanan were not party to any conspiracy (nor did they commit any unlawful acts) against Mr Azima. For these reasons, paragraph 105 is denied.

106. Paragraph 106 is denied:

- 106.1. RAKIA did not procure the hacking of Mr Azima's emails or computers or the release of the Torrents.
- 106.2. RAKIA did not cover up any of the facts regarding the hacking nor did it advance a fraudulent case concerning the circumstances in which it had learned of and acquired the hacked data.
- 106.3. RAKIA is not liable (whether "primarily" or vicariously) for any of the wrongs allegedly committed by Mr Gerrard, Mr Page, Mr del Rosso and Mr Grayson. Paragraph 35 above is repeated.

107. As to paragraph 107:

- 107.1. It is assumed that the statement that "*RAKIA did those things*" in the first sentence is a reference to the allegations in paragraph 106 of the Re-Amended Counterclaim. Those allegations are denied. Paragraph 106 above is repeated.
- 107.2. The remainder of paragraph 107 consists of the repetition of averments already made in the Re-Amended Counterclaim. RAKIA's response to the specific matters addressed at subparagraphs is as follows.
- 107.3. In relation to subparagraph a., paragraphs 28 to 29 above are repeated.
- 107.4. In relation to subparagraph b., paragraphs 3, 25, 31 to 41 above are repeated.
- 107.5. In relation to subparagraph c., paragraphs 42 to 48 above are repeated.
- 107.6. In relation to subparagraph d., paragraph 36.3 above is repeated.
- 107.7. In relation to subparagraph e., paragraphs 46 to 48 above are repeated.
- 107.8. In relation to subparagraph f., paragraphs 49 to 52 above are repeated.
- 107.9. In relation to subparagraph g., paragraph 53 to 56 above are repeated.
- 107.10. In relation to subparagraph h., paragraph 57 above is repeated.
- 107.11. In relation to subparagraph i., paragraphs 58 to 61 above are repeated.

- 107.12. In relation to subparagraph j., Mr Azima has no pleaded case as to “*RAKIA’s wider objectives*”. Insofar as this subparagraph is intended to rely on the matters pleaded at paragraphs 62 to 65 in relation to the Ruler’s “*wider objectives*”, paragraphs 62 to 65 above are repeated.
- 107.13. In relation to subparagraph k., paragraph 66 to 67 above are repeated.
- 107.14. In relation to subparagraph l., it is admitted that the first tranche of the hacked data appeared online shortly after the settlement talks with Dr Massaad ended. RAKIA is not aware of any connection between these two events.
- 107.15. In relation to subparagraph m., paragraphs 75 to 77 above are repeated.
- 107.16. In relation to subparagraph n., paragraphs 68 to 71.1 above are repeated.
- 107.17. In relation to subparagraph o., paragraphs 20, 77A, 81 and 81B above are repeated.
- 107.18. In relation to subparagraph oa.:
- (i) In relation to subparagraph i., paragraph 20 above is repeated.
 - (ii) In relation to subparagraph ii., paragraphs 21 and 80 above are repeated.
 - (iii) In relation to subparagraphs iii. and iv., paragraphs 78 to 81 above are repeated.
- 107.19. In relation to subparagraph ob., paragraphs 77A and 81B above are repeated.
- 107.20. In relation to subparagraph s., paragraphs 82 to 87.1 above are repeated.
- 107.21. In relation to subparagraph t., paragraphs 88 to 95 above are repeated.
- 107.22. In relation to subparagraph u., paragraphs 96 to 98 above are repeated.
- 107.23. In relation to subparagraph v., it is denied that RAKIA has sought to conceal or cover up the true facts.
- 107.24. Subparagraph w. is admitted.

108. Further, although RAKIA does not know who was responsible for obtaining unauthorised access to Mr Azima's emails and/or devices, it is apparent that Mr Azima was the target of long-term covert information gathering – including attempts to hack his electronic communications devices – by agents of the Government of Iran and/or Revolutionary Guards. The Government of Iran and/or the Revolutionary Guards had the means, motive and opportunity to hack and disseminate Mr Azima's electronic data. In support of this averment RAKIA will rely on the following matters:

108.1. An email sent by Ms Azadeh to Mr Azima on 4 September 2012 described how Mr Azima's electronic communications were being monitored and interfered with by agents of Iran. The email was sent after Ms Azadeh was arrested and detained for more than three months by the Iranian Government and Revolutionary Guards. In the email Ms Azadeh told Mr Azima that she had been "*accused of espionage for us [United States] by you*". She went on to warn Mr Azima that, "*your clowns and mine they are heavily infected and involved in this matter – both groups are with them*" and that, "*your maid has been paid too, they [have] pictures of your meeting in your apt and their voices*". She also warned Mr Azima that certain individuals "*are playing both ways*" and "*will feed you with the wrong info*" and that, "*u don't know your people*". She added that, "*they have recorded our voice over the phone in Dubai – your phone in dubai is infected*".

108.2. On 24 February 2016, Ms Azadeh sent Mr Azima an email which explained that within minutes of her arrest in Iran the intelligence service of the Revolutionary Guard had forced her to provide the password to her email accounts, and that she was then interrogated about HeavyLift's operations by interrogators who wanted her to confess that she was a CIA agent working with Mr Azima. Ms Azadeh stated that the Iranian interrogators had obtained access to her computer and emails and that she was eventually released after being "*made to confess that I was a CIA agent and I was working with Farhad Azima in relation to all anti-Islamic government activities supported by U.S.*"

108.3. On 1 May 2016, a spear-phishing email was sent to Mr Azima from

an IP address in Iran, indicating that Mr Azima was being actively targeted by a person or persons within Iran.

108.4. On 18 July 2016, Ms Azadeh filed a lawsuit against the Islamic Republic of Iran and the Islamic Revolutionary Guards Corp before the United States District Court for the District of Columbia. The lawsuit described how Ms Azadeh was detained in Evin Prison, Tehran where she was tortured and interrogated about Mr Azima's company, HeavyLift. Two weeks after that lawsuit was filed, the first tranche of the hacked data was published online.

108.5. On 7 March 2018, Jay Solomon, a journalist whose communications with Mr Azima were contained in the second tranche of the hacked data (entitled "*Fraud Between Farhad Azima and Jay Solomon*"), published an article in the Columbia Journalism Review in which he stated his belief that the Government of Iran had been responsible for the hacking of Mr Azima's emails and explained that he did not consider it to be a coincidence that "*the stolen data began appearing just weeks after my first story broke in August 2016 about the Obama administration's secret cash shipments to Iran*".

109. As to paragraph 108:

109.1. It is admitted that Mr Page was involved in the investigation into Dr Massaad and his associates and made the proposal set out in subparagraph a.. Paragraphs 42 to 47 above are repeated.

109.2. Subparagraph b. is admitted. Paragraph 36.3 above is repeated.

109.3. Subparagraph c. is not admitted.

109.4. Subparagraph d. is admitted. Paragraph 37 above is repeated.

109.5. Subparagraph e. is admitted. Paragraphs 96 to 98 above are repeated.

109.6. Subparagraph f. is admitted. Paragraph 36.4 above is repeated.

109.7. The Re-Amended Counterclaim has abandoned, without explanation, the contention previously advanced at subparagraph g of the Amended Counterclaim.

109.8. It is denied that Mr Page was party to any hacking, staged release of data or cover up authorised, instigated or procured by RAKIA.

110. As to paragraph 109:

- 110.1. Save that it is admitted that Mr Buchanan was a leading figure in RAKIA's investigations, subparagraph a. is denied. Paragraphs 28 to 30 above are repeated.
- 110.2. As to subparagraph b., paragraph 34 above is repeated.
- 110.3. Subparagraph c. is denied. Paragraphs 49 to 52 above are repeated.
- 110.4. Subparagraph d. is admitted. Paragraphs 62 to 65 above are repeated.
- 110.5. It is admitted that Mr Buchanan attended a meeting with Mr Azima at which Mr Gerrard was present which took place on 16 July 2016. Subparagraph e. is otherwise denied. In relation to this meeting, paragraphs 66 to 67 above are repeated.
- 110.6. Subparagraph f. is not admitted. Paragraphs 21, 80 and 81 above are repeated.
- 110.7. Subparagraph g. is denied.
- 110.8. Subparagraph h. is denied.
- 110.9. Subparagraph i. is denied. Paragraph 71 above is repeated.
- 110.10. Save that it is admitted that a number of Mr Buchanan's emails were deleted, subparagraph j. is denied. Paragraphs 82 to 87 above are repeated.
- 110.11. It is denied that Mr Buchanan was party to any hacking, staged release of data or cover up.

111. As to paragraphs 110 and 111:

- 111.1. Save that it is admitted that Mr Gerrard was closely involved in the investigations into the misappropriation of assets owned by RAKIA and the development of its strategies, paragraph 110a. is denied. Paragraphs 28 to 30 above are repeated.
- 111.2. It is denied that Mr Gerrard gave instructions to Mr Page on behalf of RAKIA. RAKIA does not believe that Mr Gerrard was privy to any wrongful activities by Mr Page or that he was party to false evidence at the First Trial.
- 111.3. It is not admitted that Mr Gerrard gave any instructions to Mr del Rosso and Vital to engage CyberRoot to hack Mr Azima's computers or emails.

- 111.4. Paragraph 100d. is denied. Paragraphs 68 to 71 above are repeated.
- 111.5. It is not admitted that Mr Gerrard was party to a false version of discovery of the Torrents in the First Trial.
- 111.6. Paragraph 100f. is admitted. Paragraphs 58 to 61 above are repeated.
- 111.7. Paragraph 100g. is denied. Paragraph 66 above is repeated.
- 111.8. Paragraph 100h. is admitted. Paragraphs 96 to 98 above are repeated.
- 111.9. Save that it is admitted that Mr Gerrard's evidence at the First Trial was inaccurate in the respects identified in his third witness statement, paragraph 100i. is not admitted. Paragraphs 88 to 95 above are repeated.
- 111.10. It is denied that Mr Gerrard was party to any hacking, staged release of data or cover up authorised, instigated or procured by RAKIA.
- 111.11. With the exception of the above, paragraph 110 is not admitted.
- 111.12. No admissions are made as to the legal effect or consequences of the relationship between Mr Gerrard and Dechert.

V. PROPER LAW

112. Paragraph 112 is admitted. The law applicable to Mr Azima's claims against RAKIA is English law.

113. As to paragraph 113:

- 113.1. It is denied that the proper law applicable to Mr Azima's claim against the Additional Defendants is the federal law of the United States of America or the state law of the State of Missouri. The law applicable to Mr Azima's claims against the Additional Defendants is English law.
- 113.2. Subparagraph a. and b. are admitted as an accurate description of the status of the Rome II Regulation ("**Rome II**") and the text of Article 4 of that Regulation.
- 113.3. Pursuant to the exclusionary provision in Article 1(2)(g) of Rome II, insofar as Mr Azima's claims against the Additional Defendants for which RAKIA is allegedly liable arise from alleged violations of Mr Azima's privacy and rights relating to personality, the law applicable to those is not determined by Rome II. Instead, the law applicable to those claims is governed by sections 11 and 12 of the

Private International Law (Miscellaneous Provisions) Act 1995 (“**PILA 1995**”). With the exception of the above, subparagraph c. is admitted.

113.4. Subparagraph d. is not admitted. Mr Azima is required to prove the existence and location of any damage allegedly caused by the publication of the hacked data, the location of his permanent residence, and the place where he conducted business.

113.5. Further and in any event, even if Missouri was the state where the “damage” occurred for the purposes of Article 4(1) of Rome II, in all the circumstances it is clear that the alleged torts are manifestly more closely connected with England than with the State of Missouri or the United States. Accordingly, pursuant to Article 4(3) of the Rome II, the law applicable to the claims is English law.

113.6. As to subparagraph e.:

(a) In relation to the aspects of Mr Azima’s claims against the Additional Defendants for which RAKIA is allegedly liable which are governed by PILA 1995, it is admitted that under the “general rule” in s. 11 of PILA 1995, the law applicable to those claims is the law in which the most significant element or elements of the events constituting the tort occurred. It is denied that the most significant element(s) of the events constituting the tort occurred in the State of Missouri. The matters pleaded at subparagraphs i.-iv. are not admitted.

(b) Further and in any event, even if the law of Missouri and/or US federal law were prima facie the applicable law under the general rule in s. 11 of PILA 1995, pursuant to s. 12 of PILA in the circumstances of the present case it is substantially more appropriate for the law applicable to those claims to be English law.

113.7. In support of the contentions at paragraphs 113.5 and 113.6 above, RAKIA will rely on the following matters:

(a) The Additional Defendants are (and were at the time of the relevant alleged events) all domiciled in England. It is not alleged that any of the Additional Defendants committed any tortious acts or omissions in the United States.

- (b) Although Mr Azima has put forward several different cases regarding how and by whom the hacking was allegedly carried out, he has never suggested that any of the persons who conducted the hacking were present in the United States when they did so. On the contrary, Mr Azima has always alleged that the persons who carried out the hacking were based outside the United States:
 - (i) At the trial, Mr Azima alleged that the hacking was carried out by Israeli operatives in Israel and that the person who created the “*Farhad Azima Exposed Again*” blog was based in the United Arab Emirates.
 - (ii) In the Re-Amended Counterclaim Mr Azima alleges that the hacking was carried out by Indian hackers in India.
 - (iii) At paragraphs 15b. and 57b. of the Re-Amended Counterclaim, Mr Azima also alleges that in 2015 and 2016 his email accounts were accessed without authorisation from India and Bulgaria.
- (c) Further, according to the expert report of Mr Azima’s forensic IT expert, Christopher Tarbell, dated 30 August 2019:
 - (i) The “*authorized connection record*” for Mr Azima’s fa@farhadazima.com email account showed that in the year before 18 November 2016 that email account had been accessed from 11 different countries including the United Kingdom, India, Bulgaria, France, Italy, Austria, Canada, Monaco, Lebanon and Jamaica.
 - (ii) Data which had been hacked from Mr Azima’s emails and computers was available from “seeders” with IP addresses in Germany and France.
- (d) Mr Azima’s Response dated 15 October 2021 to RAKIA’s Request for Further Information dated 2 September 2021 (“**Mr Azima’s RFI Response**”) states that:
 - (i) Of the 12 companies which Mr Azima claims his “*business was conducted*” through at “*the relevant time*”, nine were incorporated outside Missouri. These include companies incorporated in Gibraltar (AAA Investments

Ltd), the Cayman Islands (ALG Marine Limited and ALG Marine MYQ Limited) and the British Virgin Islands (Eurasia Aviation Holdings Limited).

- (ii) The customers of those 12 companies were “*located worldwide*”.
- (e) It is common ground that the claims against RAKIA are governed by English law pursuant to an English law and exclusive jurisdiction clause in the Settlement Agreement. The claims against the Additional Defendants are based on the same factual allegations as the claims against RAKIA. Further, the torts allegedly committed by the Additional Defendants were allegedly committed by them in their capacity as agents of RAKIA.
- (f) Mr Azima contends that RAKIA is both primarily and/or vicariously liable for the acts of Mr Gerrard, Mr Page and Mr Buchanan. In circumstances where it is common ground that all Mr Azima’s claims against RAKIA are all governed by English law, it would be inconsistent for the claims against Mr Gerrard, Mr Page and Mr Buchanan – in respect of whom RAKIA is alleged to be both primarily and vicariously liable – to be governed by a different system of law. In particular:
 - (i) Where a principal is alleged to be vicariously liable under English law for torts committed by its agent, the question of whether the acts of the agent were tortious (which is a necessary precondition to establishing vicarious liability on the part of the principal) must logically be determined by reference to English law.
 - (ii) Since it is common ground that the claims against RAKIA are exclusively governed by English law, it follows that any liability on RAKIA’s part in respect of the acts of its agents/alleged agents could only arise under English law. It follows from this that the relevant acts of those agents/alleged agents must also be governed by English law. It would be incoherent and illogical for claims in tort against RAKIA’s agents/alleged agents to

be governed by US federal law and/or Missouri state law, but claims asserting RAKIA's vicarious liability for those same alleged torts to be governed by English law.

114. As to paragraph 114:

114.1. For the reasons set out above, it is denied that the alleged torts are most closely connected with the United States or the State of Missouri and/or that, in respect of claims concerning invasions of privacy, the significance of the factors connecting those claims to the United States and to Missouri are more significant than the factors that connect those claims with other jurisdictions.

114.2. Subparagraphs a.-d. are a verbatim repetition of paragraph 112.e.i.-iv. of the Re-Amended Counterclaim. The response to those averments pleaded at paragraph 113.5 to 113.7 above is repeated.

115. As to paragraph 115:

115.1. It is admitted that as a consequence of the choice of law provision in the Settlement Agreement and the fact that the Additional Defendants were allegedly acting as RAKIA's agents, the law applicable to the claims against all of the Defendants is English law.

115.2. With the exception of the above, paragraph 115 is denied.

116. RAKIA does not plead to paragraph 116 which does not contain any relevant averment.

VI. MR AZIMA'S CLAIMS

A. CLAIMS UNDER ENGLISH LAW

1. CLAIMS FOR UNAUTHORISED ACCESS, HACKING, AND THEFT OF DATA

117. Paragraph 117 is admitted.

118. As to paragraph 118:

118.1. It is admitted that section 5 of the Data Protection Act 1998 ("**DPA**"), established territorial limitations on its application. Pursuant to section 5, the DPA only applied to the processing of personal data where the data controller was "*established in the United Kingdom and*

the data are processed in the context of that establishment” or where the data controller was established outside the United Kingdom and the European Economic Area “*but use[d] equipment in the United Kingdom for processing the data otherwise than for the purpose of transit through the United Kingdom*”. RAKIA is established in the Emirate of Ras Al Khaimah in the United Arab Emirates. It has never had any presence in the United Kingdom and never used any equipment in the United Kingdom for the purpose of processing data. Accordingly, any processing of personal data allegedly carried out by RAKIA fell outside the scope of section 5 and therefore was not subject to the provisions and requirements of the DPA.

118.2. It is denied that the territorial limitations of the DPA are inapplicable:

- (a) Section 5 of the DPA contained express territorial limitations on the scope of application of the DPA. RAKIA’s entry into a Settlement Agreement with Mr Azima which contained an English choice of law clause was neither intended to, nor capable of, disapplying or ‘waiving’ those express territorial limitations or estopping RAKIA from relying on them. Accordingly, RAKIA was at no time subject to any of the provisions or requirements contained in the DPA.
- (b) Without prejudice to the generality of that denial:
 - (i) The Settlement Agreement was entered on 2 March 2016. Mr Azima alleges that his emails and computers were first hacked on RAKIA’s instructions sometime in 2015 and that by the date of the Settlement Agreement RAKIA had acquired unauthorised access to his data and was using those data for the purposes of a conspiracy against him. It is not alleged that RAKIA was bound to comply with provisions of an English statute *before* it entered the agreement which he alleges rendered English law applicable to RAKIA.
 - (ii) Further, the choice of law clause in the Settlement Agreement provides that English law applies to “*any dispute or claim arising out of, or in connection with, it or its subject matter*”. Accordingly, under the Settlement

Agreement the trigger for the application of English law to RAKIA is the existence of a “*dispute or claim*” arising out of, or in connection with the Settlement Agreement or its subject matter. There was no such “*dispute or claim*” in existence until RAKIA issued its claim against Mr Azima on 30 September 2016. It is not alleged that by issuing that claim against Mr Azima, the provisions of the DPA became retrospectively applicable to acts which were not subject to the DPA at the time when they were allegedly carried out.

119. As to paragraph 119:

119.1. In respect of the first sentence:

- (a) It is denied that RAKIA gained unauthorised access to Mr Azima’s computers and emails, hacked or stole his data, or disclosed his data on websites.
- (b) If and insofar as it is so alleged, it is denied that RAKIA’s use of the hacked data to investigate Mr Azima’s frauds and to pursue legal redress for those frauds involved any breach of the DPA actionable by Mr Azima.

119.2. Subparagraphs a. to e. are denied. Without prejudice to the generality of that denial:

- (a) RAKIA was not responsible for hacking and making available the hacked data on the internet.
- (b) Further and in any event, RAKIA was not a “*data controller*” for the purposes of the DPA. Accordingly:
 - (i) The requirement under section 4(4) of the DPA for a “*data controller*” to comply with the data protection principles did not apply to RAKIA at any time.
 - (ii) The right under section 13 to claim compensation in respect of damage caused “*by reason of any contravention by a data controller of any of the requirements of this Act*” is therefore incapable as a matter of law of being applied against RAKIA.
- (c) Further and in any event, even if RAKIA had been a “data

controller” within the meaning of the DPA, RAKIA’s discovery of Mr Azima’s personal data on the internet and its subsequent use of that personal data to investigate his fraudulent conduct towards RAKIA and to pursue proceedings for redress in respect of that wrongdoing would not have involved any breach of the data protection principles referred to in subparagraph c. In particular:

- (i) Such processing of personal data would have been exempt from the first data protection principle on the basis that the data was being processed for the purpose of preventing or detecting crime within the meaning of section 29(1) of the DPA;
- (ii) Such processing would have been justified on the basis that it was necessary for the purposes of legitimate interests pursued by RAKIA within the meaning of paragraph 6(1) of Schedule 2 to the DPA;
- (iii) RAKIA’s acquisition and use of the personal data was for the purposes of investigating Mr Azima’s frauds and wrongdoing and pursuing legal redress (successfully) in respect of this. These purposes were specified and lawful within the meaning of paragraph 2 of Schedule 1 to the DPA.

120. As to paragraph 120:

120.1. It is admitted that the Computer Misuse Act 1990 (“**CMA**”) contains territorial limitations on its application.

120.2. RAKIA’s entry into a contract with Mr Azima which contained an English choice of law clause was neither intended to, nor capable of, disapplying or ‘waiving’ those express territorial limitations or estopping RAKIA from relying on them. Paragraph 118.2(b) above is repeated, making the necessary changes.

120.3. As a result, it is denied that the CMA has any application to the alleged hacking in this case.

121. Paragraph 121 is denied. In particular:

- 121.1. The hacking of Mr Azima's computers and emails/data did not fall within the offence established under section 1 of the CMA because it occurred beyond the jurisdictional reach of that section.
- 121.2. Further and in any event, the CMA is a criminal statute and does not create any cause of action for breach of statutory duty.
- 121.3. Accordingly, even if (which is denied) the hacking of Mr Azima's computers and emails/data constituted an offence under section 1 of the CMA, Mr Azima has no cause of action under the CMA.

2. BREACH OF CONFIDENCE AND/OR MISUSE OF PRIVATE INFORMATION

122. As to paragraph 122:

- 122.1. No admissions are made as to the nature of the information obtained through hacking and Mr Azima is put to proof as to the information or categories of information to which his claim relates.
- 122.2. In relation to each category of information to which his claim relates Mr Azima is put to proof that:
 - (a) He had a reasonable expectation of privacy in respect of such information; and/or
 - (b) That the information had the necessary quality of confidence.
- 122.3. It is specifically denied that any of the information contained in the Iniquity Documents, the RAKIA Communications and the Generic Messages was private or confidential to Mr Azima. Paragraph 6.3 above is repeated.

123. As to paragraph 123:

- 123.1. It is denied that RAKIA was responsible for the hacking or that it "infringed" Mr Azima's reasonable expectation of privacy.
- 123.2. With the exception of the above, paragraph 123 is not admitted.

124. As to paragraph 124:

- 124.1. It is denied that RAKIA was under any obligation of confidence in respect of the hacked data which it obtained from the internet where they had been made publicly available by an unknown third party or parties sometime before RAKIA first learned of their existence in August and September 2016. The hacked data were therefore all in

the public domain at the time when RAKIA acquired them.

124.2. Accordingly, even if (which is not admitted) some of the hacked data had been confidential and/or private to Mr Azima prior to their publication online, from the moment of their publication on the internet those data ceased to be confidential or private.

124.3. No admissions are made as to the position of the other Additional Defendants.

125. As to paragraph 125:

125.1. It is denied that RAKIA published the hacked data on internet sources.

125.2. It is admitted that RAKIA used the hacked data for the purposes of investigating Mr Azima's wrongdoing and brought these proceedings for fraudulent misrepresentation and unlawful means conspiracy against Mr Azima on the basis of those data. RAKIA's actions were justified in the public interest and overrode any expectation of privacy or confidence in the hacked data.

125.3. In support of this, RAKIA will rely on the Court of Appeal's express endorsement (at paragraphs 62 to 65 of its judgment) of paragraph 42.3 of RAKIA's Re-Re-Amended Reply, which stated: *"Even if ... RAKIA had been responsible for obtaining documents unlawfully from Mr Azima, the public interest in the court reaching the correct decision on the basis of all the evidence available would substantially outweigh any such unlawfulness. Accordingly, RAKIA's claim based on those documents would not constitute an abuse of process, nor would there be any basis for excluding any of those documents from the proceedings."*

125.4. Further, the use of the hacked data in proceedings before this Court is protected by absolute immunity and did not constitute any breach of Mr Azima's rights.

125.5. With the exception of the above, paragraph 125 is not admitted.

126. Paragraph 126 is not admitted.

127. As to paragraph 127:

127.1. It is denied that RAKIA acquired information through hacking or that it

misused any of Mr Azima's private or confidential information.

127.2. For these reasons, paragraph 127 is denied.

128. As to paragraph 128:

128.1. For the reasons set out above, it is denied that Mr Azima is entitled to any compensation or damages for breach of confidence or misuse of private information against RAKIA.

128.2. Further and in any event, Mr Azima is not entitled compensation or damages resulting from the publication, distribution or use of the Iniquity Documents, the RAKIA Communications or the Generic Messages or the use of the hacked data in the course of legal proceedings.

128.3. No admissions are made in respect of Mr Azima's claims for compensation and damages for breach of confidence and misuse of private information against the Additional Defendants.

128.4. It is denied that Mr Azima is entitled to any order for disgorgement. This is addressed further at paragraphs 176 and 177 below.

128.5. With the exception of the above, paragraph 128 is denied.

3. CONSPIRACY TO INJURE

129. As to paragraph 129:

129.1. It is denied that RAKIA entered into any combination or agreed course of conduct with the predominant (or any) intention of harming Mr Azima.

129.2. RAKIA repeats the response above to Sections II and III of the Re-Amended Counterclaim.

129.3. RAKIA had no involvement in the hacking or dissemination of the hacked data or the creation of websites or materials seeking to publicise the hacked data or to attack Mr Azima. Accordingly, the intention(s) of the person(s) responsible for this are unknown to RAKIA. Subparagraph a. is therefore not admitted.

129.4. The Ruler's expression of his wish to "*target*" and "*go after*" Mr Azima was not an instruction to hack Mr Azima or to engage in any other unlawful activity against him. Paragraphs 49 to 52 above are repeated.

129.5. The reference in the Project Update document to “*contain[ing] and ruin[ing]*” the plans of Mr Azima and the “*US team*” was likewise not understood by RAKIA as a reference to hacking Mr Azima or engaging in any other unlawful activity.

129.6. Mr Gerrard did not say or threaten that Mr Azima would be rendered “*collateral damage*”. Paragraphs 66 to 67 above, which explain the context and meaning of Mr Gerrard’s reference to “*collateral damage*” at the 16 July Meeting, are repeated.

129.7. Save as set out at above, paragraph 129 is not admitted.

130. As to paragraph 130:

130.1. It is denied that RAKIA instructed or otherwise procured Mr Page, Vital, Mr del Rosso and/or CyberRoot or any other person or persons to take steps to obtain Mr Azima’s private and confidential information, to ensure it became accessible on the internet and/or to procure the promotion of websites which drew attention to the exposure of such information.

130.2. The reference in the Project Update document to “*gather[ing] intelligence*” was not understood by RAKIA to be a reference to hacking or any other unlawful activity.

130.3. The Ruler’s expression of his wish for Mr Azima to be “*target[ed]*” was not an instruction to engage in hacking or any other unlawful activity. Paragraphs 49 to 52 above are repeated. Accordingly, the expression of that wish did not result in any person making, sending or receiving any communications in furtherance of a conspiracy to hack or engage in unlawful activity against Mr Azima.

130.4. It is denied that RAKIA has sought to conceal or cover up any unlawful behaviour.

130.5. Paragraph 130 is, accordingly, denied.

131. Paragraph 131 is denied.

132. Paragraph 132 is denied.

133. It is denied that RAKIA is liable to Mr Azima for the tort of conspiracy to injury

as alleged in paragraph 133.

4. UNLAWFUL MEANS CONSPIRACY

134. As to paragraph 134:

134.1. It is denied that RAKIA was party to any conspiracy against Mr Azima.

134.2. As to subparagraph a.:

- (a) It is admitted that computer hacking is unlawful under the criminal law in England and Wales, the United States and Missouri.
- (b) The presumption of equivalence between English and foreign law is a rule of English private international law which only applies to the content of foreign *civil* laws. There is no presumption that foreign *criminal* laws are the same as English criminal laws. Accordingly, no admissions are made regarding the criminal laws of any countries other than England and the United States.
- (c) In relation to the laws of England, the United States and Missouri, RAKIA's position is as set out above (in relation to the English law causes of action relied on by Mr Azima) and below (in relation to the United States and Missouri causes of action relied on by Mr Azima).

134.3. As to subparagraph b., it is denied that RAKIA committed any breach of confidence, misuse of private information or breach of any provisions of US or Missouri law. It is not admitted that any of the Additional Defendants committed any such breach of confidence, misuse of private information or breach of US or Missouri law. Paragraphs 122 to 128 above and paragraphs 139 to 166 below are repeated.

134.4. As to subparagraph c., it is denied that RAKIA has "*procured*" or "*promoted*" any unlawful websites relating to Mr Azima.

134.5. As to subparagraph d., it is denied that RAKIA instigated, procured or ratified the giving of false evidence in relation to the hacking or otherwise sought to conceal or cover up the hacking.

134.6. With the exception of the above, paragraph 134 is not admitted.

135. Save that it is denied that RAKIA was party to any conspiracy, paragraph 135 is not admitted.

136. Paragraph 136 is denied.

137. Paragraph 137 is denied.

B. CLAIMS UNDER US FEDERAL AND MISSOURI LAW

138. Paragraph 138 is denied. The law applicable to the claims against all of the Defendants is English law. Neither US Federal law nor the law of the State of Missouri is applicable to any of the claims. Paragraph 112 above is repeated. The response below to paragraphs 139 to 165 of the Re-Amended Counterclaim is without prejudice to RAKIA's primary contention that none of the provisions of US federal law and Missouri state law pleaded in those paragraphs is applicable to the claims against any of the Defendants.

1. Conspiracy to Disclose and Use Intercepted Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(d) and 2520, 18 U.S.C. §371; and Disclosure and Use of Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(c) and 2520)

139. The claims under the Wiretap Act pleaded at paragraphs 139 to 146 of the Re-Amended Counterclaim are time barred:

139.1. Under 18 U.S.C. §2520(e) the limitation period for claims under the Wiretap Act in respect of the interception, disclosure or intentional use of wire or electronic communications in violation of Chapter 119 (Wire and Electronic Communications Interception) is two years from the date upon which the claimant first had a reasonable opportunity to discover the violation.

139.2. Mr Azima was aware that his computers and emails had been hacked and that their contents had been made publicly available on the internet shortly after the first tranche of the hacked data was published online in early August 2016. On 30 September 2016, Mr Azima issued proceedings against RAKIA in the United States in which he alleged that RAKIA was responsible for that hacking and disclosure ("the **US Proceedings**"). Accordingly, it is clear that Mr Azima was aware, at the latest, by that date of the facts which he

now alleges constituted violations of the Wiretap Act.

139.3. Mr Azima's original Counterclaim dated 16 August 2019 ("the **Original Counterclaim**") did not include any claim under the Wiretap Act. The claims under the Wiretap Act were first advanced in the Amended Counterclaim served on 23 July 2021. Accordingly, the claims under the Wiretap Act pleaded at paragraphs 139 to 146 of the Re-Amended Counterclaim are all limitation barred.

139.4. The response pleaded below to the claims under the Wiretap Act is without prejudice to this limitation defence.

140. As to paragraph 139:

140.1. RAKIA did not agree or conspire with anyone to intercept Mr Azima's data by hacking or to disclose such hacked data.

140.2. Further and in any event:

(a) The provisions of the Wiretap Act set out at 18 U.S.C. §2511 and §2520 do not have extraterritorial effect and therefore do not apply to conduct by a person outside the territory of the United States. It is not alleged that any of the Defendants engaged in any conduct violating the Wiretap Act in the United States. Accordingly, even if one or more of the Defendants had committed acts in violation of the Wiretap Act, this would not fall within the scope of 18 U.S.C. §2511 and would not be capable of giving rise to any cause of action under 18 U.S.C. §2520.

(b) Civil liability under the Wiretap Act does not extend to cases where a person aids or abets unlawful interceptions carried out by other persons or conspires with other persons who carry out the unlawful interceptions. Accordingly, even if one or more of the Defendants had entered an agreement that CyberRoot or others would hack Mr Azima's data and disclose that data in violation of the Wiretap Act, the Defendants would not be civilly liable under the Wiretap Act in respect of this.

140.3. With the exception of the above, paragraph 139 is not admitted.

141. As to paragraph 140:

- 141.1. 18 U.S.C. §2511(1)(c) provides that except as otherwise specifically provided in Chapter 119, any person who intentionally discloses, or endeavours to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of that subsection, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5). The provisions of the Wiretap Act set out in 18 U.S.C. §2511 do not apply to disclosures or interceptions carried out by a person outside the territory of the United States.
- 141.2. The definitions of “*Intercept*” and “*Electronic communication*” are admitted. An “interception” only occurs for the purposes of the Wiretap Act where a communication is acquired by the defendant while it is in transmission: see, e.g., *Boudreau v. Lussier*, 901 F. 3d 65, 77 (1st Cir. 2018) and *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003). Accordingly, where a person accesses an electronic document or communication that is not in the course of being transmitted at the moment when the access occurs, this will not constitute an “interception” for the purposes of the Wiretap Act.
142. As to paragraph 141:
- 142.1. It is denied that RAKIA intercepted Mr Azima’s data.
- 142.2. Further and in any event:
- (a) Electronic communications which were sent or received *before* the hacking occurred cannot have been intercepted while they were in transmission. Similarly, electronic data documents such as photographs, videos, notes and call logs which are merely stored on a device, and not communicated electronically to/from that device, are incapable of being “intercepted” during their transmission for the purposes of the Wiretap Act. The significant majority of the hacked data comprise either documents which were sent or received before the hacking allegedly began and documents and data which were not sent or received at all. Accordingly, the acquisition of those documents and data through hacking is incapable of

constituting an “interception” within the meaning of the Wiretap Act.

- (b) Mr Azima has not identified any facts which support the assertion that the persons who hacked his email accounts acquired emails sent to or from those accounts during the transmission of such emails.
- (c) As set out at paragraph 140.2 above, the Wiretap Act does not have extraterritorial application and therefore even if one or more of the Defendants had intercepted Mr Azima’s emails, the Wiretap Act is inapplicable.

142.3. With the exception of the above, paragraph 141 is not admitted.

143. Save that it is denied that RAKIA disclosed Mr Azima’s data by publishing intercepted data on the Torrents or that it added new links to his data as alleged, paragraph 142 is not admitted.

144. As to paragraph 143:

144.1. It is denied that RAKIA was party to any conspiracy to use hacked data to damage Mr Azima.

144.2. RAKIA discovered the hacked data on the internet and subsequently used it for the purposes of investigating and successfully pursuing proceedings against Mr Azima for his serious frauds and other wrongdoing. This was a lawful and legitimate use of the hacked data, and RAKIA denies any liability arising from such use. Without prejudice to the generality of that denial, RAKIA’s use of the hacked data for this purpose was and is protected by the First Amendment to the Constitution of the United States.

144.3. With the exception of the above, paragraph 143 is not admitted.

145. As to paragraphs 144 to 145:

145.1. It is denied that RAKIA was party to the hacking or dissemination of Mr Azima’s data.

145.2. It is not admitted that Mr Azima has suffered damage as alleged.

145.3. Further and in any event, the Defendants’ alleged acquisition and dissemination of Mr Azima’s data would not constitute interception

within the meaning of the Wiretap Act and would not fall within the scope of the civil remedies established under the Wiretap Act. Paragraphs 141 and 142 above are repeated.

145.4. With the exception of the above, paragraphs 144 and 145 are not admitted.

146. As to paragraph 146:

146.1. It is not admitted that the hacked data continues to be available on WeTransfer.

146.2. It is denied that RAKIA was responsible for (or in any way involved with) the creation of WeTransfer links which allegedly made that data available online.

146.3. It is not admitted that Mr Azima has been caused any continuing damage as alleged.

2. Misappropriation of Trade Secrets, 18 U.S.C. §§ 1831, 1832, 1836

147. Mr Azima's claims under the Defend Trade Secrets Act ("**DTSA**") are time barred:

147.1. Under 18 U.S.C. §1836(d) the limitation period for claims under the DTSA is three years from the date upon which the misappropriation which the action relates to is discovered or by the exercise of reasonable diligence should have been discovered. A continuing misappropriation constitutes a single claim of misappropriation.

147.2. Mr Azima was aware that his computers and emails had been hacked and that their contents had been disseminated on the internet shortly after the first tranche of the hacked data was published online in early August 2016. On 30 September 2016, Mr Azima issued the US Proceedings against RAKIA in which he alleged that RAKIA was responsible for the hacking and dissemination and was aware of the alleged misappropriation, at the latest, by that date.

147.3. Mr Azima's Original Counterclaim served on 16 August 2019 did not include any claim under the DTSA. The claims under the DTSA were first advanced in the Amended Counterclaim served on 23 July 2021, nearly five years after Mr Azima first accused RAKIA of being

responsible for the hacking and dissemination. Accordingly, the claims under the DTSA pleaded at paragraphs 146 to 149 are time barred.

147.4. The response pleaded below to the claims under the DTSA is without prejudice to this limitation defence.

148. Further and in any event, the DTSA did not come into force until 11 May 2016. Federal courts in the United States have held that the DTSA has no application to alleged misappropriations which occurred before that date: *TFOR LLC v Virtustream, Inc* 2:16-cv-602 (E.D. Va. Jun. 22, 2017). Accordingly, insofar as Mr Azima's claim is based on acts of hacking and/or dissemination which occurred prior to 11 May 2016, the DTSA has no possible application to that claim.

149. As to paragraph 147:

149.1. The terms of 18 U.S.C. §§1832(a)(1) and 1836(b)(1) pleaded at paragraph 147 are admitted.

149.2. It is denied that 18 U.S.C. §§1831 and 1832 create any cause of action. These provisions create a criminal offence, but do not establish any civil remedy or cause of action.

149.3. Further and in any event, there is no liability under the DTSA in respect of a defendant that has conspired, but not directly participated in, the misappropriation of the trade secret: see *Masoud v. Suliman*, 816 F. Supp. 2d 77, 80 (D.D.C. 2011); *Bennett v. Wolf*, 2019 WL 3802466, at 1 (W.D. Wis. Aug. 13, 2019); *Lopez v. MUFG Union Bank, N.A.*, 2016 WL 9686990, at 6 (C.D. Cal. Mar. 30, 2016); *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 271 F. Supp. 3d 835, 842–43 (E.D. Va. 2017).

150. As to paragraph 148:

150.1. It is not admitted that Mr Azima's email accounts stored "*trade secrets*" including "*highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, or contacts for important business relationship*" as

alleged and Mr Azima is put to proof that the hacked data contain such information and that such information constituted “trade secrets” for the purposes of 18 U.S.C. §1836(b)(1) on the basis that the information had independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person, and that he took reasonable measures to keep such information secret.

150.2. Without prejudice to the non-admission in paragraph 150.1 above, the alleged trade secrets identified in Table 2 to Mr Azima's RFI Response all relate to businesses conducted through companies. Accordingly, the alleged misappropriation of those alleged trade secrets is incapable of giving rise to any cause of action actionable by Mr Azima. In particular:

- (a) Under 18 U.S.C. §1836(b)(1) the right to bring a civil action for misappropriation of a trade secret is limited to the “owner” of the trade secret. For these purposes, the “owner” is the company to which the trade secret relates, not the shareholder or director of the company.
- (b) Further and in any event, the rule in Prudential Assurance Company v Newman Industries Ltd (No. 2) [1982] Ch 204 precludes Mr Azima from bringing a claim in respect of a loss allegedly suffered as a result of a wrong done to a company in which he is a shareholder. Accordingly, Mr Azima is unable to bring a claim in respect of losses which he has allegedly suffered as a result of an alleged misappropriation of a trade secret belonging to a business in which he is a shareholder.

150.3. Further and in any event, it is denied (if it is so alleged) that the contents of any of the Iniquity Documents, the RAKIA Communications or the Generic Messages were capable of constituting qualifying “trade secrets” for the purposes of the DTSA.

151. The allegations in paragraph 149 are denied insofar as they relate to RAKIA and are not admitted insofar as they relate to the other Defendants. Further and in any event, it is Mr Azima's case that each of the Additional Defendants was an agent of RAKIA. Under both United States federal law and the law

of the State of Missouri, it is not possible for a conspiracy to exist between an agent and a principal or between agents of a principal. Accordingly, the averment that RAKIA is liable for a conspiracy entered with and/or between its alleged agents is legally incoherent and the Re-Amended Counterclaim contains no valid plea of conspiracy under US law.

152. As to paragraph 150:

- 152.1. It is not admitted that any trade secret and/or confidential information belonging to Mr Azima was misappropriated. Paragraph 150 above is repeated.
- 152.2. It is not admitted that Mr Azima suffered any damage as a result of the alleged conspiracy and the hacking.
- 152.3. Further and in any event, any loss of business goodwill or harm to Mr Azima's business was the consequence of the public revelation of Mr Azima's serious frauds and other unlawful conduct. Mr Azima is not entitled to any financial or non-financial remedy in respect of losses caused by the exposure of his own wrongdoing.

3. The United States Computer Fraud and Abuse Act

153. Mr Azima's claims under the Computer Fraud and Abuse Act ("**CFAA**") are time barred:

- 153.1. Under 18 U.S.C. §1030(g) the limitation period for claims under the CFAA is two years from the date of the act complained of or of the date of the discovery of the damage.
- 153.2. Mr Azima was aware that his computers and emails had been hacked and that their contents had been made publicly available on the internet shortly after the first tranche of the hacked data was published online in early August 2016. On 30 September 2016, Mr Azima issued the US Proceedings in which he alleged that RAKIA was responsible for that hacking and disclosure and for the resulting damage which the hacking and disclosure allegedly caused. Accordingly, it is clear that Mr Azima was aware, at the latest, by that date of the facts which he now alleges constituted violations of the CFAA.
- 153.3. Mr Azima did not plead any claim under the CFAA against RAKIA in

these proceedings until 16 August 2019. Those claims were brought more than two years after both the date of the hacking and publication and the date when Mr Azima first became aware of those facts. Accordingly, the claims under the CFAA pleaded at paragraphs 151 to 154 of the Re-Amended Counterclaim are limitation barred.

153.4. The response pleaded below to the claims under the CFAA is without prejudice to this limitation defence.

154. As to paragraph 151:

154.1. It is admitted that pursuant to 18 U.S.C. §1030(g) of the CFAA any person who suffers damage or loss by reason of a violation of that section may maintain a civil action against the violator.

154.2. It is admitted that 18 U.S.C. §1030(e)(2)(B) (not 18 U.S.C. §1030(e)(2)(8)) provides that a “protected computer” includes a computer which is used in or affecting interstate or foreign commerce or communication.

154.3. Subparagraph b. is not admitted. Mr Azima is required to plead and prove the specific computers which he alleges were accessed without his authorisation and that they qualify as a “protected computer” under 18 U.S.C. § 1030(e)(2)(B).

154.4. Subparagraph c. is admitted.

154.5. Subparagraph d. is denied in relation to RAKIA and is otherwise not admitted.

154.6. Subparagraph e. is denied.

155. As to paragraph 152:

155.1. It is admitted that it is contrary to the CFAA intentionally to access a protected computer without authorisation and, as a result of such conduct, recklessly cause damage.

155.2. RAKIA did not hack Mr Azima’s devices or alter Mr Azima’s data on those devices, nor did it instruct or authorise anyone else to do so. With the exception of the above, subparagraph a. is not admitted.

155.3. As to subparagraph b.:

(a) It is admitted that 18 U.S.C. §1030(g) provides that a person

who suffers damage or loss (as defined in §1030(e)(8), (11)) by reason of a violation of §1030 may bring a civil claim for compensatory damages against the violator, but only if able to show a loss of at least \$5,000: see *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004).

- (b) It is denied that that Mr Azima has any cause of action for compensation under 18 U.S.C. §1030 against RAKIA.
- (c) Further, even if (which is denied) Mr Azima had a cause of action for compensation under 18 U.S.C. §1030 against RAKIA or any of the Additional Defendants, pursuant to 18 U.S.C. §1030(g) the claim would be limited to compensation for “*damage*” or “*loss*” as defined by that section:
 - (i) “*Damage*” means “*any impairment to the integrity or availability of data, a program, a system, information*”: U.S.C. 18 §1030(e)(8).
 - (ii) “*Loss*” means “*any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service*”: 18 U.S.C. §1030(e)(11).
- (d) Subparagraph b. is otherwise not admitted.

156. Paragraph 153 is not admitted. Mr Azima is required to prove which of his computers were infected and how, which of his computers were disposed of and replaced and why that was necessary, what disruption to his business took place, and that such disruption was attributable to the impairment of his computers.

157. Paragraph 154 is denied insofar as it relates to RAKIA and is otherwise not admitted.

4. The Missouri Computer Tampering Act

158. Paragraph 155 is admitted. The provisions of the Missouri Computer Tampering Act (“**MCTA**”) do not apply extraterritorially. In support of this averment, RAKIA will rely on the principle that, absent express text to the contrary, Missouri statutes are presumed to have no extraterritorial effect. Since it is not alleged that any of the Defendants were present in Missouri at the time when they committed the alleged acts on which the claims under the MCTA are based, it follows that the MCTA has no application to those alleged acts.
159. Paragraph 156 is admitted, save that section 537.525 of the Revised Statutes of Missouri does not state that an owner “*is entitled to recover*” compensatory damages, but rather provides that such an owner “*may bring a civil action*” for compensatory damages.
160. Save that it is denied that the MCTA applies extraterritorially, paragraph 157 is not admitted.
161. Save that it is denied that RAKIA was party to any computer tampering or that it is jointly and severally liable with any other persons in respect of this, paragraph 158 is not admitted.

5. Invasion of Privacy Torts – Intrusion on the Seclusion of Another

162. As to paragraphs 159 and 160:
- 162.1. It is denied that RAKIA was a party to the hacking. It is therefore denied that RAKIA is liable to Mr Azima for the tort of invasion of privacy (intrusion on the seclusion of another) as alleged at paragraphs 159 to 160 or at all.
- 162.2. It is not admitted that the hacked data included any secret and private subject matter. It is denied (if it is alleged) that the Iniquity Documents, the RAKIA Communications or the Generic Messages were secret and private or that Mr Azima had a right to keep such documents (or information about such documents) secret. Paragraph 6.3 above is repeated.
- 162.3. Although paragraph 160 contends that Mr Azima is entitled to “*special damages*”, no special damages are pleaded in the Re-

Amended Counterclaim and no Schedule of Special Damage has been served by Mr Azima.

162.4. It is not admitted that Mr Azima has suffered any mental distress as a result of any invasion of his privacy. Without prejudice to the generality of that non-admission:

- (a) Distress must be medically significant in order to be capable of giving rise to any entitlement to damages under this cause of action;
- (b) Any distress which Mr Azima has suffered is much more likely to be the consequence of the public exposure of true facts concerning his own fraudulent conduct and wrongdoing, for which he is not entitled to recover any damages.

162.5. With the exception of the above, paragraphs 159 and 160 are not admitted.

6. Invasion of Privacy - Public Disclosure of Private Facts

163. As to paragraphs 161 and 162:

163.1. It is denied that RAKIA was a party to the hacking and dissemination of Mr Azima's data. Accordingly:

- (a) It is denied that RAKIA was a party to any of the matters described at paragraph 161a.-d.
- (b) It is denied that RAKIA is liable (whether jointly and severally or otherwise) to Mr Azima for the tort of invasion of privacy (public disclosure of private facts).

163.2. It is denied that the hacked data contained private matters in which the public had no legitimate concern. There was a strong and legitimate concern in the public exposure of Mr Azima's serious frauds and other wrongdoing and therefore there was a strong and legitimate public concern in the publication of the Iniquity Documents. The Iniquity Data concerned newsworthy matters of public concern and the publication of those matters is protected by the First Amendment to the United States Constitution.

163.3. As to the claim for damages for harm to Mr Azima's privacy interests:

- (a) Mr Azima has failed to provide any particulars regarding (i) any shame or humiliation which he allegedly suffered; and (ii)

why a person of ordinary sensibilities would have experienced such shame or humiliation.

- (b) According to Mr Azima, the hacked data included a large number of documents and communications concerning his businesses and various records of his phone usage (such as call histories, contacts and notes). It is inherently unlikely that the publication of unremarkable documents, communications and records of this nature would cause any shame or humiliation to a person of ordinary sensibilities.
- (c) Mr Azima is not entitled to recover any damages for shame or humiliation caused by the public exposure of true facts concerning his own fraudulent conduct and wrongdoing. Any such shame or humiliation is the consequence of Mr Azima's own dishonesty and wrongdoing, rather than any actionable invasion of privacy.

163.4. No admissions are made as to the nature and extent of Mr Azima's recoverable damages.

163.5. Although paragraph 162 avers that Mr Azima is entitled to damages for "*specific damages*" caused by the disclosure of the alleged private facts, no claim for special damages is pleaded in the Re-Amended Counterclaim and no Schedule of Special Damage has been served by Mr Azima.

163.6. It is not admitted that Mr Azima has suffered any mental distress as a result of any invasion of his privacy. Without prejudice to the generality of that non-admission:

- (a) Distress must be medically significant in order to be capable of giving rise to any entitlement to damages under this cause of action;
- (b) Any distress which Mr Azima has suffered was the consequence of the public exposure of true facts concerning his own fraudulent conduct and wrongdoing, for which he is not entitled to recover any damages.

163.7. With the exception of the above, paragraphs 161 and 162 are not admitted.

7. Tortious Interference with Business Relationship and Business Expectancy

164. It is unclear what “*business*” “*conducted*” by Mr Azima paragraph 163 is intended to refer to. Save that it is admitted that RAKIA was aware that Mr Azima had various business interests, paragraph 163 is not admitted.

165. As to paragraph 164:

165.1. It is denied that RAKIA was a party to the hacking and dissemination of Mr Azima’s data. Accordingly, it is denied that RAKIA did any of the things listed at subparagraphs a. to e.

165.2. Without prejudice to that denial, the Re-Amended Counterclaim and Mr Azima’s RFI Response:

- (a) do not provide any particulars as to the way(s) or respect(s) in which Mr Azima’s business and business expectancy were allegedly interfered with;
- (b) do not identify the “*improper means*” whose alleged “*employment*” is said to have given rise to the alleged tort; and
- (c) do not provide any particulars as to the “*business relationships*” which were allegedly severed or the business expectancy which was allegedly lost.

165.3. Further and in any event:

- (a) The alleged severance of business relationships, interference with business and loss of business expectancy all concern business conducted through companies owned by Mr Azima. The rule in Prudential Assurance Company v Newman Industries Ltd (No. 2) [1982] Ch 204 precludes Mr Azima from bringing a claim in respect of a loss of business allegedly suffered as a result of a wrong done to a company in which he is a shareholder. The claims at paragraphs 163 to 164 of the Re-Amended Counterclaim are therefore barred by that rule.
- (b) Mr Azima is in any event not entitled to recover any damages for loss of business expectancy or severance of business relationships caused by the public exposure of the true facts concerning his own fraudulent conduct and wrongdoing. Any

such loss or severance is the consequence of Mr Azima's own dishonesty and wrongdoing, rather than any actionable tortious interference with business relationships or business expectancy.

8. Conspiracy

166. As to paragraph 166:

166.1. It is denied that RAKIA was a party to the hacking and dissemination of Mr Azima's data. Accordingly, it is denied that RAKIA was party to a civil conspiracy under Missouri law as alleged in paragraph 165.

166.2. Further and in any event, it is Mr Azima's case that each of the Additional Defendants was an agent of RAKIA. Under both United States federal law and the law of the State of Missouri, it is not possible for a conspiracy to exist between an agent and a principal or between agents of a principal. Accordingly, the averment that RAKIA is liable for a conspiracy entered with and/or between its alleged agents is legally incoherent and the Re-Amended Counterclaim contains no valid plea of conspiracy under Missouri law.

166.3. With the exception of the above, paragraph 165 is not admitted.

C. LOSS, DAMAGE AND OTHER RELIEF

167. It is denied that Mr Azima has suffered any loss and damage for which RAKIA is liable to pay compensation. Without prejudice to the denial of liability set out above:

167.1. The acquisition and publication of the Iniquity Documents, which demonstrated Mr Azima's extensive fraudulent conduct (including serious frauds perpetrated against RAKIA) is not capable of giving rise to any cause of action against RAKIA. It follows that even if (which is denied) RAKIA was responsible for the hacking, RAKIA would not be liable for any pecuniary or non-pecuniary damage which was caused by the publication of the Iniquity Documents.

167.2. The Re-Amended Counterclaim does not attempt to distinguish between (1) loss/damage caused by the acquisition and publication of the Iniquity Documents; and (2) loss/damage caused by the

acquisition and publication of other material which does not constitute evidence of Mr Azima's serious frauds and wrongdoing. The Re-Amended Counterclaim therefore fails to identify any alleged damage which was caused by an allegedly actionable publication of private and confidential material, as opposed to a non-actionable publication of non-private and non-confidential material.

167.3. Any alleged pecuniary or non-pecuniary damage suffered by Mr Azima is more likely to have been the consequence of the public exposure of true facts concerning Mr Azima's own fraudulent and unlawful conduct, rather than the acquisition and publication of other material which did not contain evidence of such misconduct. In support of this averment, RAKIA will rely on the following matters:

- (a) Documents demonstrating that Mr Azima had orchestrated and participated in numerous frauds and other serious wrongdoing were inherently more likely to damage Mr Azima's reputation and to attract significant adverse attention and media coverage than documents which contained information of a more anodyne character.
- (b) Mr Azima's Original Counterclaim:
 - (i) alleged that Mr Azima had suffered serious reputational and financial damage as a result of the publication of false statements accusing him of fraud and other wrongdoing; and
 - (ii) sought substantial damages for the torts of defamation, malicious falsehood, injurious falsehood and commercial disparagement in respect of those allegedly false statements.
- (c) The allegations and claims described in paragraph (b) above demonstrate that the loss and damage which Mr Azima claims to have suffered was caused principally or exclusively by the public exposure of (true) facts about Mr Azima's own fraudulent conduct and wrongdoing. Those allegations have been abandoned in the Re-Amended Counterclaim in response to the High Court's findings that Mr Azima had engaged in seriously fraudulent conduct towards RAKIA. The

abandonment of those allegations in the Re-Amended Counterclaim reflects the fact that Mr Azima is not entitled to any remedy in respect of loss and damage caused by the public exposure of true facts about his own fraudulent conduct and wrongdoing.

167.4 Further, insofar as the losses which Mr Azima claims to have suffered were either losses suffered by companies of which he is a shareholder, or comprise a reduction in the value of Mr Azima's shareholdings in such companies and/or a diminution in the distributions he receives by virtue of such shareholdings, the rule in Prudential Assurance Company v Newman Industries Ltd (No. 2) [1982] Ch 204 (affirmed by the Supreme Court in Sevilleja v Marex Financial Ltd [2021] AC 39) precludes Mr Azima from recovering any damages in respect of those losses in these proceedings.

1. Pecuniary Losses

168. Paragraph 166 is denied insofar as it relates to RAKIA and is otherwise not admitted.

169. Paragraph 167 is not admitted. Without prejudice to that non-admission:

169.1. The first draft of the Amended Counterclaim pleaded at paragraph 167(a) that as a result of the hacking Mr Azima "*required professional assistance to investigate it*" and alleged that he had incurred expenditure of \$183,000 in respect of "*professional services required (from ZP Consultants LLC) to investigate and mitigate the hacking*". Following receipt of that draft, on 15 June 2021 RAKIA's solicitors wrote to Mr Azima's solicitors expressing serious concern that Mr Azima had not previously divulged the alleged involvement of ZP Consultants LLC in investigating and mitigating the hacking, nor disclosed any documents produced or held on his behalf by that company (despite such documents plainly falling within the scope of Mr Azima's standard disclosure obligations). Mr Azima's solicitors failed to provide any explanation for the absence of any previous mention of, or disclosure of any documents relating to, ZP Consultants LLC. Instead, on 2 July 2021, Mr Azima's solicitors

served an amended draft of the Amended Counterclaim which retained the averment regarding ZP Consultants LLC, save that the amount of that alleged expenditure had been changed (without explanation) from \$183,000 to \$60,000. This contention was maintained in the Amended Counterclaim served on 23 July 2021. In its Request for Further Information dated 2 September 2021, RAKIA sought full particulars of the “*professional services*” provided by ZP Consultants LLC. Mr Azima did not provide any such particulars. Instead, on 30 September 2021 Mr Azima served a draft Re-Amended Counterclaim which entirely abandoned (without any explanation) the contentions that:

- (i) he had required professional assistance to investigate the hacking; and
- (ii) he had incurred costs of \$60,000 in engaging ZP Consultants LLC to investigate and mitigate the hacking.

169.2. If and insofar as the alleged expenditures referred to at paragraph 167b.-c. of the Amended Counterclaim were not incurred by Mr Azima personally and/or concerned the replacement of (or the provision of protective software for) computers which were not owned by Mr Azima personally, it is denied that Mr Azima is entitled to recover damages in respect of this. In this regard, it is noted that Mr Azima’s RFI Response states that of the four computers which were allegedly replaced, two were “*located at the office of ALG Transportation*” and one was located “*at Mr Ray Adams’ home office in Leawood, Kansas*”. It is therefore to be inferred that those computers were owned by ALG Transportation Inc. and/or Mr Adams, rather than Mr Azima.

170. As to paragraph 168:

170.1. It is not admitted that Mr Azima has suffered extensive damage to his business. Paragraph 167 above is repeated.

170.2. The fact that Mr Azima is seeking to challenge the Court of Appeal’s dismissal of his appeal in respect of RAKIA’s claims has no logical bearing upon his ability to particularise the extent of his alleged pecuniary losses:

- (a) Unless and until the Supreme Court allows Mr Azima's appeal, the Judge's findings in respect of RAKIA's claims stand and Mr Azima is required to plead his Counterclaim on the basis of those findings.
 - (b) In any event, Mr Azima's appeal to the Supreme Court does not seek to challenge the findings of Iniquity against him. Accordingly, even if the Supreme Court were to allow his appeal, this would have no effect on his ability to particularise his alleged pecuniary losses.
- 170.3. Similarly, there is no logical connection between the extent of the damage that Mr Azima claims his business has suffered, and the determination of the parties who were responsible for the hacking and their reasons for doing it. Mr Azima's ability to particularise his alleged pecuniary damage is in no way dependent upon his ability to plead or establish who was responsible for hacking or how and why those persons carried out that hacking.
- 170.4. With the exception of the above, paragraph 168 is denied.
- 170.5. Further and in any event, even if (which is denied) Mr Azima has suffered extensive damage to his business, since all such business was conducted through companies owned by Mr Azima, he is precluded by the rule in Prudential Assurance Company v Newman Industries Ltd (No. 2) [1982] Ch 204 from pursuing any personal claim in respect of such damage or losses caused by such damage.

2. Non-Pecuniary Losses

171. As to paragraph 169:

- 171.1. It is not admitted that Mr Azima suffered any distress or emotional harm as a result of the unlawful publication of the hacked data.
- 171.2. If (which is not admitted) Mr Azima did suffer distress or emotional harm as a result of the publication of the hacked data, this was solely or predominantly caused by the revelation of his own fraudulent and unlawful conduct. Mr Azima is not entitled to damages for distress or emotional harm caused by the exposure of true facts regarding his own serious wrongdoing.
- 171.3. Further and in any event, it is denied that Mr Azima is entitled to any

damages for distress or emotional harm caused by the publication of information or data in which he had no reasonable expectation of privacy or confidence.

3. Exemplary Damages

172. Paragraph 170 is denied insofar as it relates to RAKIA and is otherwise not admitted.

173. As to paragraph 171:

173.1. RAKIA was the investment authority of RAK. It is not an “*organ*” of RAK in any other sense.

173.2. The second sentence is denied. None of the Additional Defendants was a servant of the government of RAK.

173.3. In relation to the third sentence, it is assumed that the reference to “*paragraph 34*” is a typographical error and is in fact intended to refer to paragraph 35 of the Re-Amended Counterclaim. It is denied that RAKIA was liable for any of the alleged wrongdoing by the Additional Defendants. Paragraph 35 above is repeated.

173.4. It is denied that RAKIA engaged in actions which were oppressive, arbitrary or unconstitutional (or that any such actions were committed by others in circumstances which rendered the actions attributable to RAKIA). The fourth sentence is otherwise not admitted.

173.5. Subparagraphs a. to c. are denied insofar as they relate to RAKIA and are otherwise not admitted.

174. As to paragraph 172:

174.1. It is denied that RAKIA engaged in any wrongdoing towards Mr Azima (whether through Mr Buchanan, Mr Gerrard or otherwise) and denied it calculated to make a profit or other gain that would exceed the amount of any compensation potentially payable to Mr Azima or that it would undermine efforts to bring attention to alleged human rights abuses in RAK.

174.2. As to subparagraph b., it is denied that Mr Page received any remuneration from RAKIA. Save as aforesaid, subparagraph b. is

not admitted.

174.3. Save that it is admitted that Mr Buchanan received substantial remuneration, subparagraph c. is denied.

174.4. Save that it is admitted that Dechert received substantial remuneration (of at least \$1 million per month during some periods of their retainer), subparagraph d. is denied. It is specifically denied that Mr Gerrard received any remuneration from RAKIA.

174.5. The remuneration referred to at subparagraphs 174.2 to 174.4 above was in consideration of lawful services. RAKIA did not make any payment to any of the Additional Defendants in consideration of any unlawful acquisition, misuse or dissemination of Mr Azima's confidential data.

174.6. With the exception of the above, paragraph 172 is not admitted.

175. Paragraph 173 is denied:

175.1. In respect of RAKIA, for the reasons set out above:

- (a) RAKIA is not liable for any of the torts alleged in the Re-Amended Counterclaim.
- (b) Even if (which is denied) RAKIA was liable for one or more of those alleged torts, the conditions for making an award of exemplary damages against RAKIA are not met.

175.2. In respect of the Additional Defendants, for the reasons set out above:

- (a) It is not admitted that those Defendants are liable for any of the torts alleged in the Re-Amended Counterclaim.
- (b) Even if (which is not admitted) those Defendants are liable for one or more of the alleged torts, the conditions for making an award of exemplary damages against them are not met.

175.3. Further, even if (which is denied) the conditions for making an award of exemplary damages against one of the Defendants were met, the fact that those conditions are not met in respect of one or more of the other Defendants means that exemplary damages are unavailable as a matter of law against any of the Defendants.

175.4. Further and in any event, exemplary damages are only available as a matter of law in respect of causes of action in tort. It follows that

exemplary damages are unavailable as a matter of law in respect of Mr Azima's claims for breach of confidence.

4. Disgorgement

176. As to paragraph 174:

176.1. It is admitted that the Additional Defendants received the remuneration pleaded in paragraph 174 above.

176.2. The remuneration paid to the Additional Defendants was exclusively in consideration of lawful services. RAKIA did not make any payment to any of the Additional Defendants in consideration of any unlawful acquisition, misuse or dissemination of Mr Azima's confidential data.

176.3. With the exception of the above, paragraph 174 is not admitted.

177. Paragraph 175 is denied. Even if (which is denied) the remuneration paid to the Additional Defendants was for or in consideration of them unlawfully acquiring, misusing or disseminating Mr Azima's confidential data, that remuneration would not have been at the expense of Mr Azima and there would be no basis for ordering the Additional Defendants to account to Mr Azima in respect of some or all of that remuneration.

5. Interest

178. As to paragraph 176:

178.1. The reference to "*the Defendant*" at paragraph 176 is assumed to refer to Mr Azima.

178.2. It is denied that Mr Azima is entitled to any award of interest against RAKIA.

6. Injunctive Relief

179. As to paragraph 177:

179.1. Mr Azima is not entitled to any injunctive relief against RAKIA.

179.2. RAKIA is not able to remove or procure the removal of the websites, torrents, WeTransfer links or other internet sources containing statements about Mr Azima or providing means for his data to be accessed by others.

179.3. RAKIA has no knowledge of the extent of the hacking or the parties

involved.

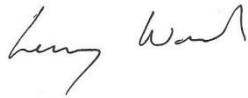
7. Orders made by Deputy Judge Lenon QC

180. The first sentence of paragraph 178 is denied. There is no basis on which it would be appropriate for the Court to vary the orders made by the Judge concerning interest and costs in respect of RAKIA's claims against Mr Azima.

HUGH TOMLINSON QC
EDWARD CRAVEN

Statement of truth

The Defendant to the Counterclaim believes that the facts stated in this Defence to Counterclaim are true. The Defendant to the Counterclaim understands that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.



Signed:

Date: 19 November 2021

Name: Lucy Ward

Position: Partner, Stewarts Law LLP